SAMSUNG

CY-SWR1100
www.samsung.com

Wireless Router

CY-SWR1100 User's Manual

Safety Information

Safety Warnings

To reduce the risk of electric shock, do not remove the cover (or back) of the router.
No user serviceable parts are inside. Refer to qualified service personnel.

		
This symbol indicates "dangerous voltage" inside the product that presents a risk of electric shock or personal injury.	Caution: To prevent electric shock, match wide blade of plug to the wide slot, fully insert.	This symbol indicates important instructions accompanying the product.

Warning

- To reduce the risk of fire or electric shock, do not expose this apparatus to rain or moisture.

Caution

- Do not expose this device to dripping or splashing. Do not place objects filled with liquids, such as vases, on the products
- To turn this device off completely you must pull its plug out of the wall socket. To ensure you can unplug the product quickly if necessary, only plug the product into an easily accessible outlet.
- Only connect this device to an AC outlet with a protective grounding connection.

Precautions

- Ensure that the AC power supply in your house complies with the requirements listed on the identification schecker located on the back of this device.
- Install your device horizontally or vertically on a suitable piece of furniture or on a wall using the included wall mounting kit with enough space around it for proper ventilation (7.5~10cm)
- Do not place the device on an amplifier or other piece of equipment which may become hot.
- Do not stack anything on top of the device.
- To disconnect the device completely from the power supply, remove its plug from the wall outlet. We strongly recommend unplugging the device if you are going to leave it unused for a long period of time.
- During thunderstorms, disconnect the AC plug from the wall outlet. Voltage spikes due to lightning could damage the device.
- Do not expose the device to direct sunlight or other heat sources. Exposure to heat sources can cause the device to overheat and malfunction.
- Protect the device from moisture, excess heat and equipment creating strong magnetic or electric fields (i.e. speakers.).
- Unplug the device from the wall socket if it malfunctions.
- Your device is not intended for industrial use. It is for personal use only.
- Condensation may occur in the device if is has been stored in cold temperatures. If you transport the device during the winter, wait approximately 2 hours until the device has reached room temperature before using.

Table of Contents

Getting Started

Package Contents

What's in the box:

- Wireless 802.11a/b/g/n Dual Band Router
- Power Adapter with extra Power Cable
- Ethernet Cable
- CD-ROM (with installation software and manuals)
- Quick Installation Guide
- Stand
- Wall Mount Kit

System Requirements

Network Requirements:

- 10/100/1000Mbps Ethernet LAN adapter
- 802.11a/b/g/n Wireless Adapter
- Ethernet-based Cable or DSL Modem

Computer Requirements:

- Window 7/Vista/XP (with SP3)
- 10/100/1000Mbps Ethernet LAN adapter
- CD-ROM drive

Software Requirements:

- Operating System like Microsoft Windows, Mac OS, or Linux
- Browser like Internet Explorer (6 or higher), Mozilla Firefox (3.0 or higher), Safari (3.0 or higher), or Chrome (2.0 or higher)

About this Product

The Samsung CY-SWR1100 is designed to provide you with advanced networking functionality and the highest quality network connections.

Features

The Samsung CY-SWR1100 wireless router is packed with all the features you'd expect in an internet Wireless router and more : It gives you features unique to Samsung products - features you'll find nowhere else.

- **INTERNET CONNECTIVITY.** In conjunction with a DSL or Cable Modem, this device can act as the Internet Gateway to your local network. It is compatible with PPPoE, PPTP, L2TP, Static IP connections and Dynamic IP Connections.(DHCP).
- **WIRELESS LAN FUNCTIONALITY**. This router supports the full 802.11n protocol. It also provides WMM, Automatic Fallback, RF Output Level Control, the latest Wireless Security requirements, WPS and much more.
- **NETWORKING**. This router is equipped with 4 LAN ports running at 10/100/1000Mbps, and 1 Internet port running at 10/100/1000Mbps. It can handle a network of up to 1000 MAC addresses.
- **MULTICASTING.** This device supports IGMPv2.
- **DHCP**. This device supports both Server and Client functionality.
- **QUALITY OF SERVICE**. You can create QoS rules to shape traffic based on weight or priority. You can also manage IP Pools based on application port numbers.
- **ADVANCED SECURITY**. The Samsung router supports a list of security features such as Network Filtering, Access Control, Website Filtering, Inbound Filtering and SPI.
- **IPv6**. Ahead of its time, the router provides both local IPv6 support and IPv6 Internet Connection support.
- **MORE**. Other features include DDNS, System Checking, Firmware Updates, Email Settings (for notification), and Schedules.

- **UNIQUE SAMSUNG FEATURES:**

  * **ONE FOOT CONNECTION.** Lets you to connect your Samsung TV/AV/Touch Control automatically to this router in seconds using the OFC connection method.

  * **PLUG & ACCESS**. Gives you a quick and easy method to connect this router to Samsung TVs using a USB memory stick.

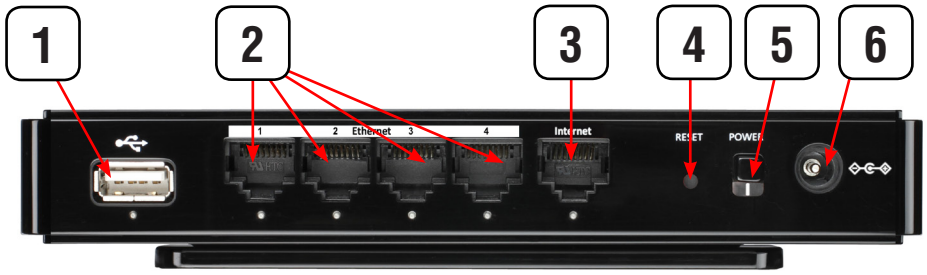
  * **SAMSUNG PRIORITY QoS.** Identifies Samsung TVs and Blu-ray players in your network and gives them higher network priority. Perfect for video streaming to your Samsung TV.

Description

Front View

1	POWER Light	A solid blue light indicates a proper connection to the power supply.
2	INTERNET Light	A solid blue light indicates the PPP negotiation has successfully completed.
3	2.4Ghz Light	A solid light indicates that the 2.4GHz wireless segment is ready. This LED blinks during wireless data transmission.
4	5Ghz Light	A solid light indicates that the 5.0GHz wireless segment is ready. This LED blinks during wireless data transmission.
5	WPS Button	Press the WPS button for 2 seconds to initiate the WPS wireless connection process. WPS is an easy method for connecting devices to your network. A flashing light indicates that the WPS connection is being established. A solid light, on for 5 seconds, indicates that the WPS client has successfully been added to the network.

Back View



1	USB PORT	The USB port is used for WPS enabled Wireless USB adapters. It is also used for the **Plug & Access** feature.
2	LAN PORTS	The four LAN ports are used for 10/100/1000Mbps LAN connections.
3	INTERNET PORT	The Internet (WAN) port is used to connect to DSL/Cable modems and similar devices.
4	RESET BUTTON	Press the Reset button for more than 5 seconds to restore the router to its original factory default settings.
5	POWER SWITCH	The Power Switch turns the router on and off.
6	POWER RECEPTOR	Receptor for the supplied power adapter.

Installation

This section will walk you through the installation process. Placement of the router is very important. Do not place the router in an enclosed area such as a closet, cabinet, attic or garage.

Pre-Installation Considerations

- Note that you must configure the router with the computer that was last connected directly to your modem.
- You can only connect this router to the Ethernet port on your modem. If you are now using the USB connection, you must turn off your modem when you install this router, disconnect the USB cable and connect an Ethernet cable to the Internet port on the router and the Ethernet port on your modem, and then turn the modem back on. In some cases, you may need to call your ISP to change connection types (USB to Ethernet).
- If you have DSL and are connecting via PPPoE, make sure you disable or uninstall any PPPoE software such as WinPoet, Broadjump, or Enternet 300 from your computer or you will not be able to connect to the Internet.
- When running the Setup Wizard from the CD, make sure the computer you are running the CD from is connected to the Internet and online or the wizard will not work. If you have disconnected any hardware, reconnect your computer to the modem and make sure you are online.

Wireless Installation Considerations

The wireless router lets you access your network using a wireless connection from anywhere within its operating range. Keep in mind, however, that the number, thickness and location of walls, ceilings, or other objects that the wireless signals must pass through, may limit the range. Typical ranges vary depending on the types of materials and background RF (radio frequency) noise in your home or business. The key to maximizing wireless range is to follow these basic guidelines:

- Keep the number of walls and ceilings between the router and other network devices to a minimum - each wall or ceiling can reduce your adapter's range from 3-90 feet (1-30 meters.) Position your devices so that the number of walls or ceilings is minimized.
- Be aware of the direct line between network devices. A wall that is 1.5 feet thick (.5 meters), at a 45-degree angle appears to be almost 3 feet (1 meter) thick. At a 2-degree angle it appears over 42 feet (14 meters) thick! Position devices so that the signal will travel straight through a wall or ceiling (instead of at an angle) for better reception.
- Building Materials make a difference. A solid metal door or aluminum studs may have a negative effect on range. Try to position access points, wireless routers, and computers so that the signal passes through drywall or open doorways. Materials and objects such as glass, steel, metal, walls with insulation, water (fish tanks), mirrors, file cabinets, brick, and concrete will degrade your wireless signal.
- Keep your product at least 3-6 feet (or 1-2 meters) away from electrical devices or appliances that generate RF noise.
- If you are using 2.4GHz cordless phones or X-10 (wireless products such as ceiling fans, lights, and home security systems), your wireless connection may degrade dramatically or drop completely. Make sure your 2.4GHz phone base is as far away from your wireless devices as possible. The base transmits a signal even if the phone in not in use.
- You can wall mount this router (see page 9). If you wall mount the modem, all the considerations above apply.

Connect to Cable/DSL/Satellite Modem

To access your network and the internet through the router, you must physically connect the router to your cable, DSL, or satellite modem or to another router.

To connect the router to a cable/DSL/satellite modem, follow these steps

1. Place the router in an open and central location. Do not plug the power adapter into the router.
2. Unplug the modem's power adapter. Shut down your computer.
3. Unplug the Ethernet cable (that connects your computer to your modem) from your computer and place it into the Internet port on the router.
4. Plug an Ethernet cable into one of the four LAN ports on the router. Plug the other end into the Ethernet port on your computer.
5. Plug in your modem. Wait for the modem to boot (about 30 seconds).
6. Plug the power adapter into the router and connect the adapter to an outlet or power strip.
7. Use the power switch to turn on the router. Wait about 30 seconds for the router to boot.
8. Turn on your computer.
9. For the information you need to continue the installation, go to "Required Network Information" on page 10.

Connecting to Another Router

If you are connecting the router to another router to use as a wireless access point and/or switch, you must do the following before connecting the router to your network:

- Disable UPnP™
- Disable DHCP
- Change the LAN IP address to an available address on your network. The LAN ports on the router cannot accept a DHCP address from your other router.

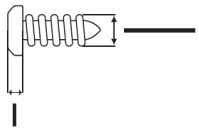
To connect to another router, please follow these steps:

1. Plug the power adapter into the router and connect the adapter to an outlet or power strip.
2. Turn on the router, and then connect one of your computers to the router's LAN port using an Ethernet cable. Make sure your IP address on the computer is 192.168.0.xxx (where xxx is between 2 and 254). If you need to change the settings, write down your existing settings before making any changes. In most cases, your computer should be set to receive an IP address automatically in which case you will not have to do anything to your computer.
3. Open a web browser and enter http://192.168.0.1 and press Enter. When the login window appears, set You name to '**admin**' and leave the password box empty. Click **Login** to continue.
4. Click Advanced and then Click Advanced Network. Uncheck the Enable UPnP checkbox. Click Save Settings to continue.
5. Click Setup, and then Click Network Settings. Uncheck the Enable DHCP Server checkbox. Click Save Settings to continue.
6. Under Router Settings, enter an available IP address and the subnet mask of your network. Click Save Settings to save your settings. Use this new IP address to access the configuration utility of the router in the future. Close the browser and change your computer's IP settings back to the original values as in Step 2.
7. Disconnect the Ethernet cable from the router and reconnect your computer to your network.
8. Connect an Ethernet cable to one of the LAN ports of the router and connect it to your other router. Do not plug anything into the Internet (WAN) port of the router.
9. You can now use the other 3 LAN ports to connect other Ethernet devices and computers. To configure your wireless network, open a web browser and enter the IP address you assigned to the router. Refer to the Configuration and Wireless Security sections for more information on setting up your wireless network.

Wall-Mounting

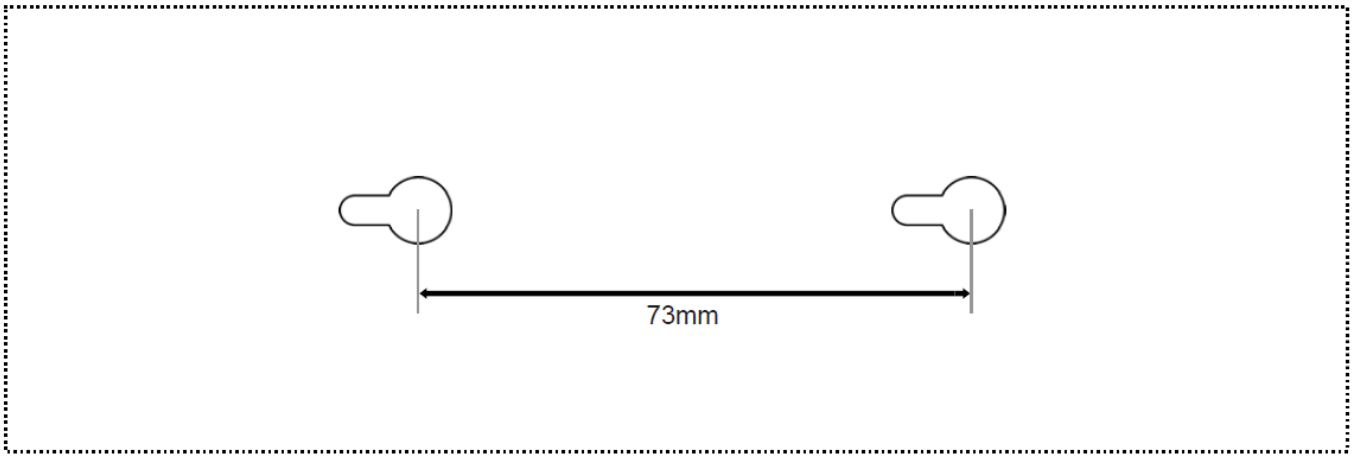
You can mount this router on a wall. The stand, included in the package, has two wall-mount slots at the bottom. The distance between these slots is exactly 73mm apart (about 3.24 inches). Use the template below to help you drill these holes precisely. Also included in the packaging are two screw, which you'll need to mount this router to a wall. If you are mounting the router on dry wall, we recommend using mollies to secure the screws in the wall.

Note: Samsung is not responsible for damages incurred by unsecured wall-mounting hardware.

Suggested Mounting Hardware	
 4-5 mm	 1-1.5 mm

To mount the router to a wall, following these steps:

1. Determine where you want to mount the Router. Make sure that the wall is smooth, flat, dry, and sturdy. Also make sure the location is within reach of an electrical outlet and the modem or other router you intend to connect this router to.
2. Tape the template below to the wall.
3. Drill two holes into the wall where indicated on the template. Make sure the holes are 73mm apart.
4. Remove the template from the wall.
5. Insert mollies into each hole, and then insert a screw into each mollie, leaving 3mm of its head exposed.
   Note : If you have drilled a hole into a stud, you do not need to insert a mollie into that hole.
6. Position the Stand so the wall-mount slots line up with the two screws.
7. Place the wall-mount slots over the screws and slide the Router to the right until the screws fit snugly into the wall-mount slots.



Print this page at 100% size. Cut along the dotted line, and place on the wall to drill precise spacing.

Required Network Information

Before you can configure your router's network settings, you need to gather the following information about your network:

- **ADDRESS MODE.** Does your modem connect to the Internet using a Dynamic (DHCP) address or does your Internet Provider (IP) require a Static address? If your IP requires a Static address, you must get all the address parameters and then enter them manually when you configure your router. These parameters include IP Address, Subnet Mask, Gateway Address, and Primary DNS Address or Server IP Address. You can get the parameter information from your IP. If your modem connects using a Dynamic address, your IP provides those parameters automatically, though you may need your Host Name to configure the router.
- **CONNECTION PROTOCOL.** Does your modem connect to the Internet using PPPoE, PPTP, or L2TP? If it does, you will need protocol specific information to configure your router. The information required for each protocol is listed in the table below:

Protocol	Required Information
PPPoE	• User Name • Password PPPoE is commonly used by DSL providers. In most cases, these providers use Dynamic (DHCP) addresses. If your provider uses Static addresses, you will also need to provide the IP address.
PPTP	• User Name • Password In most cases, PPTP protocol providers use Dynamic (DHCP) addresses. If your provider uses Static addresses, you will also need to provide the IP Address, Subnet Mask, Gateway Address, and Server IP Address.
L2TP	• User Name • Password In most cases, L2TP protocol providers use Dynamic (DHCP) addresses. If your provider uses Static addresses, you will also need to provide the IP Address, Subnet Mask, Gateway Address, and Server IP Address.

If you get your Internet from a Cable company, in most cases you will not need to get Connection Protocol information, but you will need to find out if your Address Mode is Dynamic (DHCP) or Static. If it is Dynamic, you may need your Host Name. If it is static, you will need to get the IP Address, Subnet Mask, Gateway Address, and DNS Address to configure your router. You can get this information from your Internet Provider.

Once you have the required network information, go to "Connecting to the Web UI" on page 11.

Connecting to the Web UI

After you have physically connected your router to your modem or another router, you must set up the router to access your network. The first step in this process is connecting to the Web UI in the router. To connect to the Web UI, you'll need the Router Default information listed below.

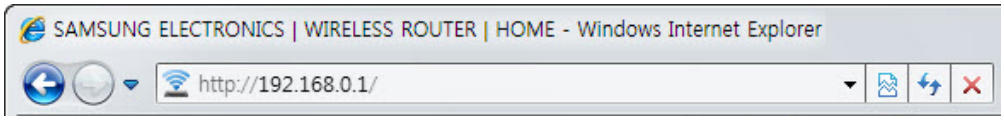
Router's Defaults

The router's default values are as follows:

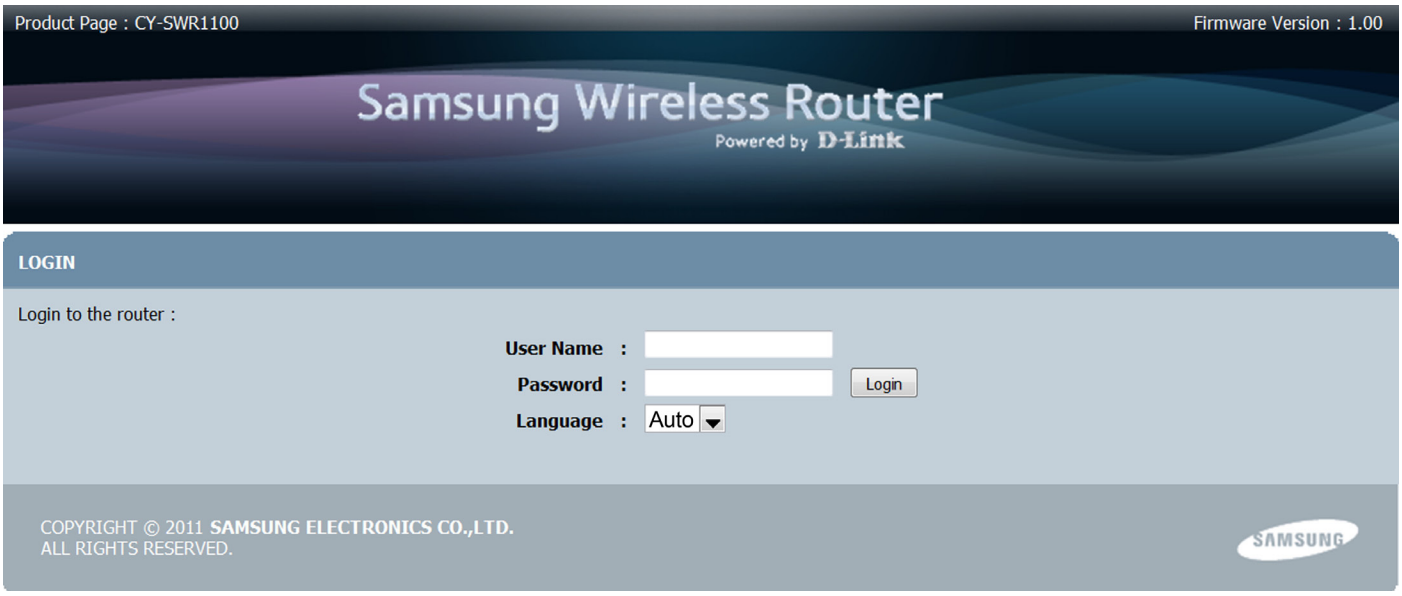
IP Address:	192.168.0.1
Username:	admin
Password:	(blank)

Open your Browser

To connect the router's Web UI, you'll need to use your Internet Browser. Open your Internet browser (Internet Explorer, Firefox, etc.) and enter the router's default IP address - 192.168.0.1 - into the address bar. If you connected your router to another router, you must enter the IP address you assigned the router in Step 6 in the Connecting to Another Router procedure.



After entering the IP address, press <enter> or Click the '**Go**' option. The login page appears:



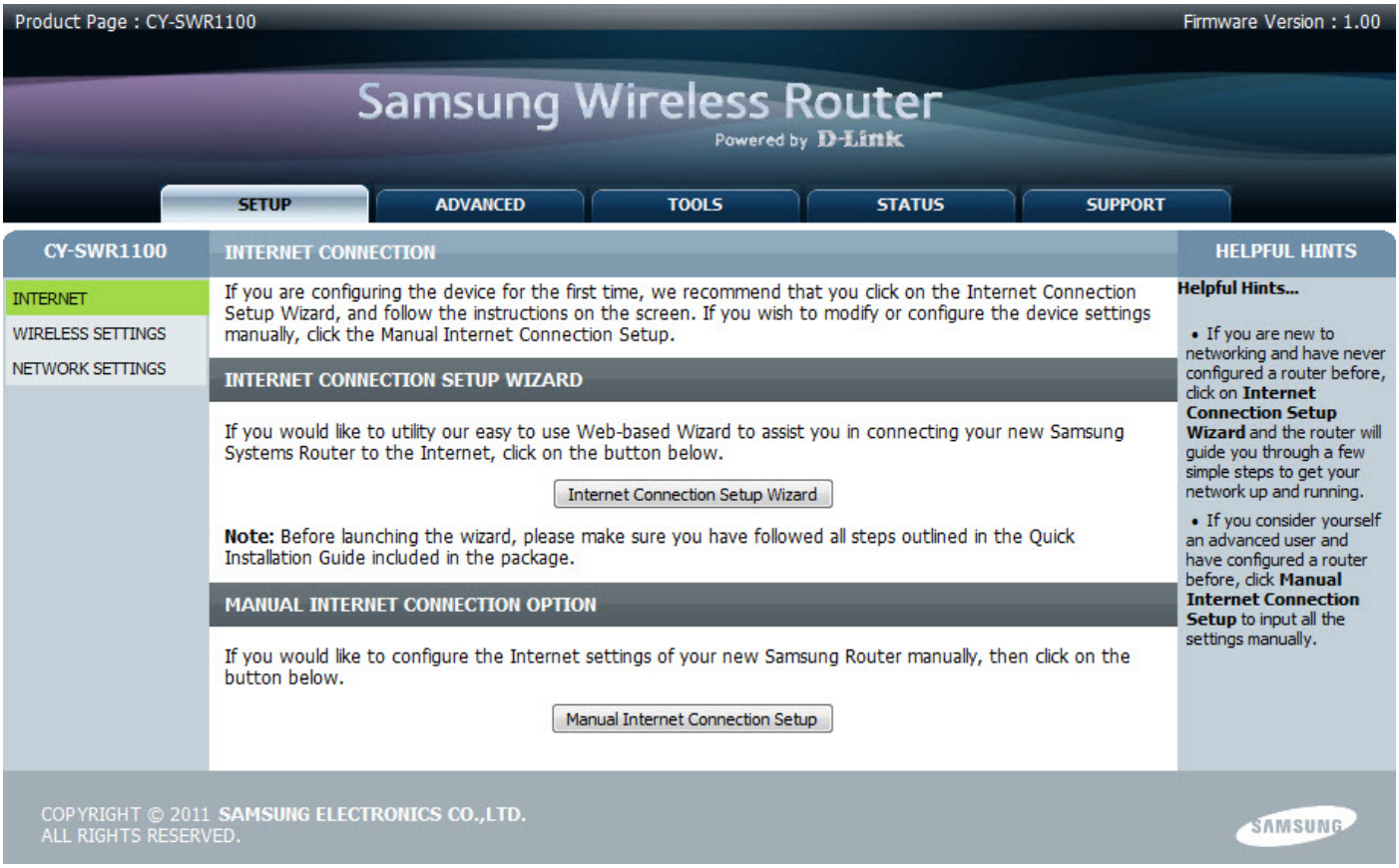
The router supports English, Spanish and French. Select the language you want to use from the Language drop down list.

Enter the default username - admin - into You Name field. Leave the Password field blank, and then Click the **Login** button. The Main Web User Intface screen appears.

Web User Interface

The Web User Interface has five tabs on top. When opened, each tab displays a series of page names on the left side. You Click the tab to open the tab screen and Click the page name on the left side to access a page. Below is the Setup screen and a table describing the functions available on each screen.

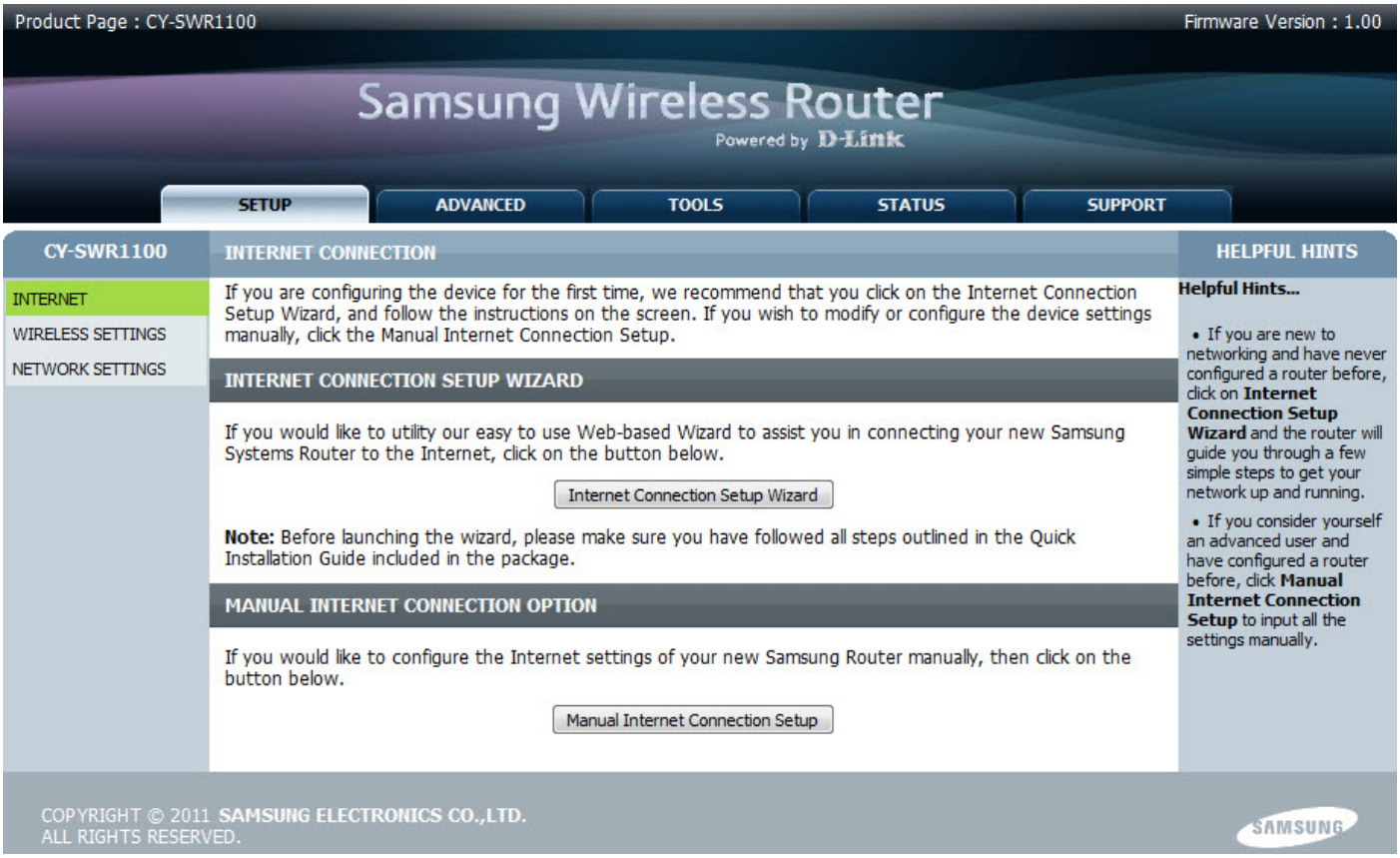
To continue setting up the router to access your network, go to Set Up Tab on the following page.



The Samsung Wireless router Web UI provides five categories to edit.

Setup:	On the Setup screen, you can configure the router's basic features to operate properly on your network. These features include Internet Connectivity, Local Area Network Connectivity, and Wireless Connectivity.
Advanced:	On the Advanced screen, you can configure the router's more advanced features. These features include Port Forwarding, Firewall settings, Quality of Service settings, and more.
Tools:	On the Tools screen, you can configure features that are related to the router itself. These features include the time settings, login accounts, firmware update and more.
Status:	On the Status screen, you can view information regarding the configuration and functionality of the router. The information includes WAN, LAN and Wireless configurations, System, Firewall and Router logs, and more.
Support:	On the Support screen, you have access to a comprehensive Help feature that contains information about each screen and page that exists on this device. The Help feature provides a basic description of all the router's parameter and the uses for each.

Setup Tab



Through the Setup tab, you can configure the router's basic features to function properly on your network. These features include Internet Connectivity, Local Area Network Connectivity, and Wireless Connectivity.

You can access the following pages from the Setup Tab:

- **Internet:** For configuring the Internet settings of the router.
- **Wireless Settings:** For configuring the Wireless settings of the router.
- **Network Settings:** For configuring the Network settings of this router.

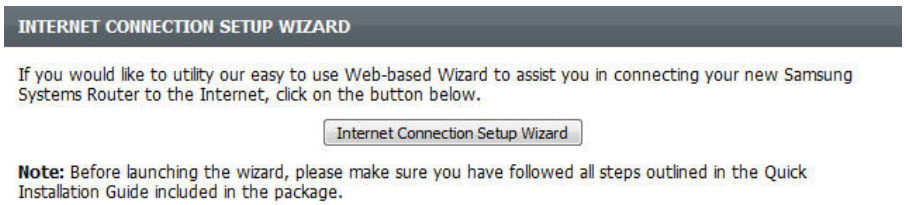
You can also launch the Internet Connection Setup Wizard and access the Manual Internet Connection Setup pages.

To configure the Internet settings of your router using the Connection Wizard, go to "Internet Connection Wizard" on page 14. We recommend most people use the Connection Wizard.

If you are a more experienced user, and you want to set up your router manually, go to "Internet - Manual Internet Connection" on page 20.

Internet - Wizard

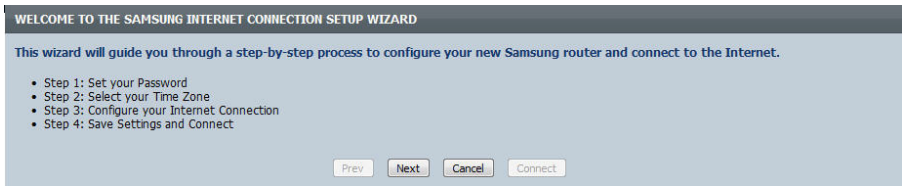
When configuring the CY-SWR1100 for the first time, we recommend that you use the **Internet Connection Setup Wizard**, and follow the instructions on the screen. This wizard is designed to provide a quick and easy way to configure the router's Internet Connectivity.



To begin the quick and easy Internet Connection Wizard, Click the **Internet Connection Setup Wizard** button on the Setup Screen. The Wizard Welcome window appears listing the four steps of the setup process:

Step 1: Set Your **Password**.
Step 2: Select Your **Time Zone**.
Step 3: Configure Your **Internet Connection**.
Step 4: Save Settings and Connect.

An illustration of the screen is below.



On all the screens in the Wizard, you can Click the **Prev** button to return to the previous window and Click the **Next** button to continue to the next window. Click the **Cancel** button to discard the changes made and return to the Internet home page.

Click the Next button now to go to Step 1, Set Your Password.

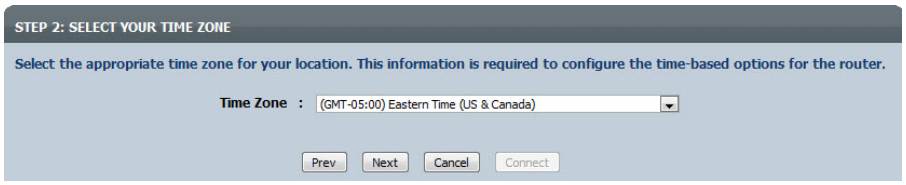
STEP 1: Set Your Password

By default, the new Samsung Router does not have a password configured for administrator access to the Web-based configuration pages. To secure your router, enter a password into the Password field, and then re-enter the password in the Verify Password field.

When done, Click the **Next** button to continue to Step 2, Select Your Time Zone.

STEP 2: Select Your **Time Zone**

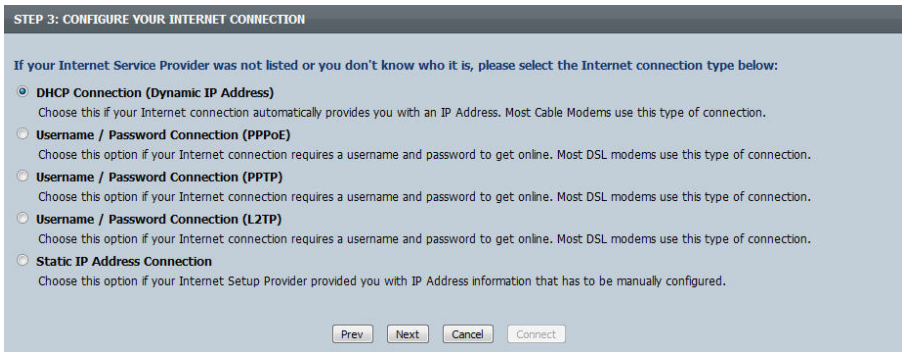
Click the arrow next to the Time Zone field and select the appropriate time zone for your location from the drop down list. This information is required to configure the time-based options for the router.



When done, Click the **Next** button to continue to Step 3, Configure Your Internet Connection.

STEP 3: Configure Your **Internet Connection**

The Configure Your Internet Connection page presents five options. See the illustration below. Using the network information you gathered previously, select the option that matches your Address Mode and/or Connection Protocol. Instructions for selecting the correct option are in the table below the illustration.



Option	Instructions
Dynamic IP Address:	Choose if your Internet connection is not a PPPoE, PPTP, or L2TP connection and uses a Dynamic IP address. Most Cable Modems use this type of connection.
PPPoE	Choose if you have a PPPoE Internet connection. Most DSL modems use this type of connection.
PPTP	Choose if you have a PPTP Internet connection.
L2TP	Choose if you have a L2TP Internet connection.
Static IP Address:	Choose if your Internet connection is not a PPPoE, PPTP, or L2TP connection and it requires a Static IP address.

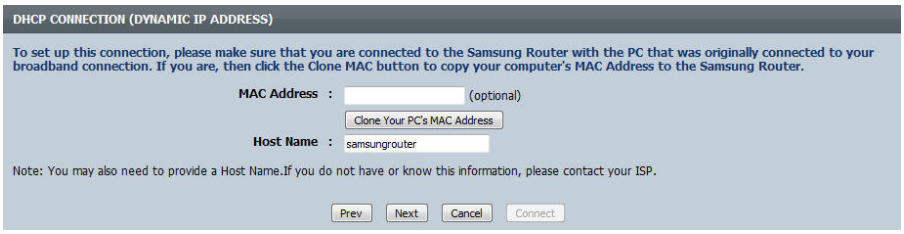
After you have selected the correct option, Click Next. The screen that corresponds to your selection appears. The screens are explained on the following pages:

"Dynamic IP Address Connection" on page 16
"PPPoE Connection" on page 16
"PPTP Connection" on page 17
"L2TP Connection" on page 17
"Static IP Address Connection" on page 18

Go to the appropriate page.

Dynamic IP Address Connection

After you select **Dynamic IP Address**, the following page appears:



Parameter	Instructions
MAC Address:	If you know the MAC address of your Internet gateway, enter it here. This is the MAC address of the device through which the router will access the Internet. If you're not sure, leave the MAC Address field blank.
Host Name:	Enter the Host Name here. The Host Name is the name assigned to your computer by your Internet Service Provider (ISP). If you do not know this information, please contact your ISP.

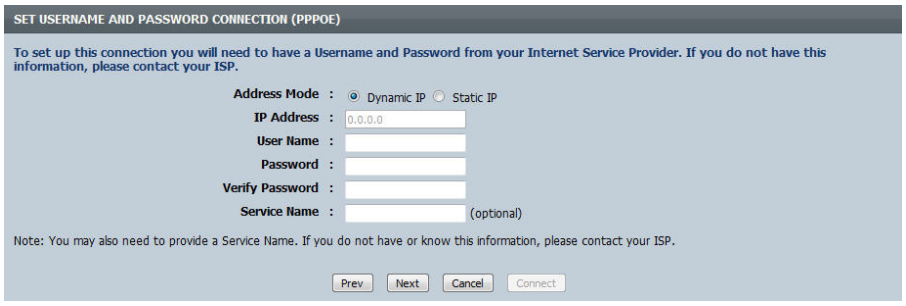
The page also has a Clone Button. If the configuration PC - the PC connected to the router - also acts as the Internet gateway, then Click the **Clone Your PC's MAC Address** button to copy the PC's MAC address into the space provided. If you're not sure, leave the MAC Address field blank.

Click **Next** to continue to Step 4 and go to page 19.

Click the **Cancel** button to discard the changes and return to the Internet home page.

PPPoE Connection

After you select **PPPoE**, the following page appears:



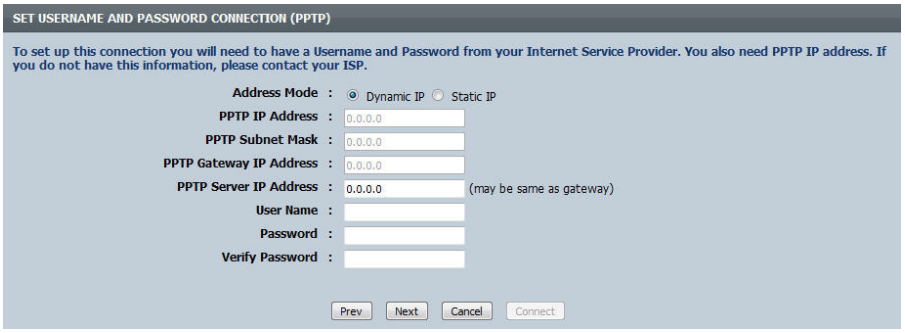
Parameter	Instructions
Address Mode:	You must select either Dynamic or Static IP address from the Address Mode drop down list. PPPoE usually requires a Dynamic IP address.
IP Address:	If you selected Static Address, enter the PPPoE IP address here. This option is only available if you selected Static IP.
User Name:	Enter your PPPoE account user name here.
Password:	Enter your PPPoE account password here.
Verify Password:	Re-enter your PPPoE account password here.
Service Name:	This optional field lets you enter a service name to identify this Internet connection.

Click **Next** to continue to Step 4 and go to page 19.

Click the **Cancel** button to discard the changes and return to the Internet home page.

PPTP Connection

After you select **PPTP**, the following page appears:



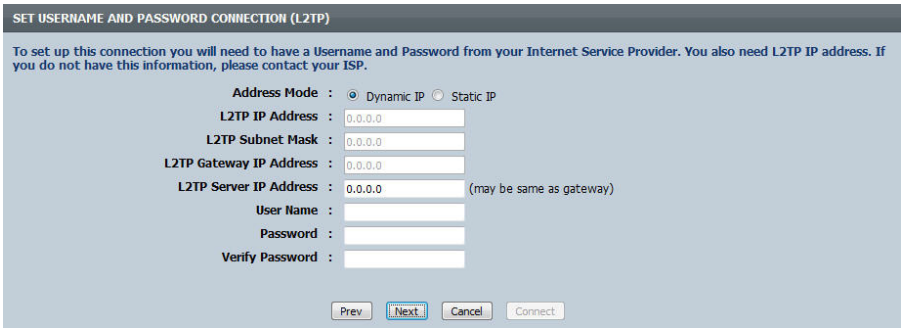
Parameter	Instructions
Address Mode:	You must select either Dynamic or Static IP address from the Address Mode drop down list. PPTP usual requires a Dynamic IP address.
PPTP IP Address:	If you selected Static Address, enter the PPTP IP address here. This option is only available if you selected Static IP.
PPTP Subnet Mask:	If you selected Static Address, enter the PPTP Subnet Mask here.
PPTP Gateway IP Address:	If you selected Static Address, enter the PPTP Gateway IP address here.
PPTP Server IP Address:	Enter the PPTP Server IP address here. This is normally the same a the PPTP Gateway IP address.
User Name:	Enter your PPTP username here.
Password:	Enter your PPTP password here.
Verify Password:	Re-enter your PPTP password here.

Click **Next** to continue to Step 4 and go to page 19.

Click the **Cancel** button to discard the changes and return to the Internet home page.

L2TP Connection

After you select **L2TP**, the following page appears:

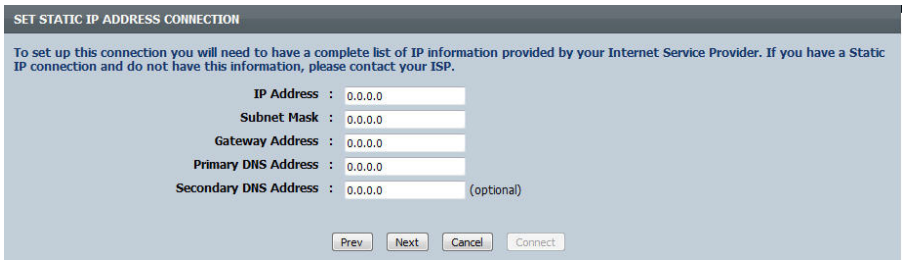


Parameter	Instructions
Address Mode:	You must select either Dynamic or Static IP address from the Address Mode drop down list. L2TP usual requires a Dynamic IP address.
L2TP IP Address:	If you selected Static Address, enter the L2TP IP address here. This option is only available if you selected Static IP.
L2TP Subnet Mask:	If you selected Static Address, enter the L2TP Subnet Mask here.
L2TP Gateway IP Address:	If you selected Static Address, enter the L2TP Gateway IP address here.
L2TP Server IP Address:	Enter the L2TP Server IP address here. This is normally the same a the L2TP Gateway IP address.
User Name:	Enter your L2TP username here.
Password:	Enter your L2TP password here.
Verify Password:	Re-enter the L2TP password used here.

Click **Next** to continue to Step 4 and go to page 19.
Click the **Cancel** button to discard the changes and return to the Internet home page.

Static IP Address Connection

After you select **Static IP Address**, the following page appears:

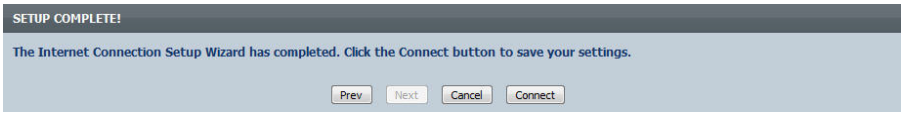


Parameter	Instructions
IP Address:	Enter the Static IP address provided by the ISP here.
Subnet Mask:	Enter the Subnet Mask provided by the ISP here.
Gateway Address:	Enter the Gateway IP address provided by the ISP here.
Primary DNS Address:	Enter the Primary DNS IP address here.
Secondary DNS Address:	Enter the Secondary DNS IP address here. This field is normally optional. Only one DNS address is required for a functional Internet connection, but using a second DNS address provides more stability.

Click **Next** to continue to Step 4 and go to page 19.
Click the **Cancel** button to discard the changes and return to the Internet home page.

Step 4

The Internet Connection Setup Wizard is complete. Click the **Connect** button to save your settings.



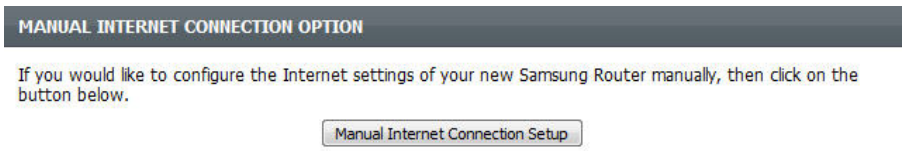
Click the **Cancel** button to discard the changes and return to the Internet home page.

After you Click the **Connect** button, the following window appears. The router saves the settings and returns to the main Internet page.

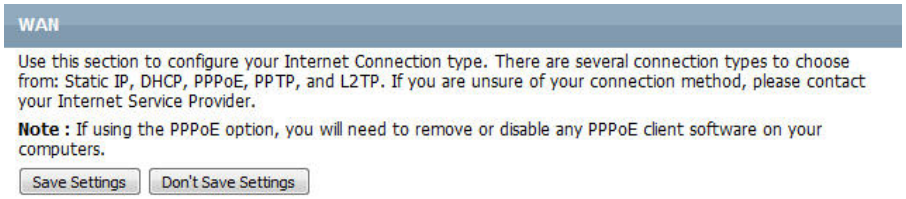
If you have successfully run the Connection Setup Wizard, you are now ready to configure your router for wireless operation. To begin, go to "Wireless Settings" on page 29.

Internet - Manual Internet Connection

The Manual Internet Connection pages let more advanced users setup the router's connection to the Internet manually. To access the Manual Internet Connection page, click the **Manual Internet Connection Setup** button.



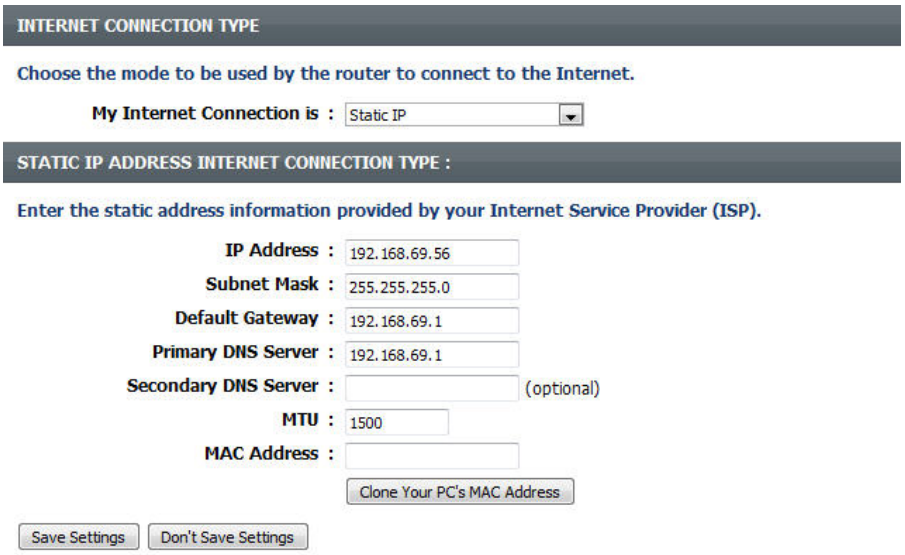
On the Manual Internet Connection page, you can configure multiple Internet Connection setup parameters by Internet Connection Type (Static IP, Dynamic IP, PPPoE, etc.).



At any point, you can save the settings you've configured on this page by Clicking the **Save Settings** button. If you choose to discard the changes, click the **Don't Save Settings** button.

Internet Connection Type: Static IP

Select Static IP from the drop-down menu if all the Internet IP information provided to you by your ISP was in a written, printed, or verbal form. You will need to key in the IP address, subnet mask, gateway address, and DNS address(es) provided to you by your ISP in the fields provided. Each IP address entered in the fields must be in the appropriate IP form, which is four octets separated by a dot (1111.2222.3333.4444). The Router will not accept an address if it is not in this format.



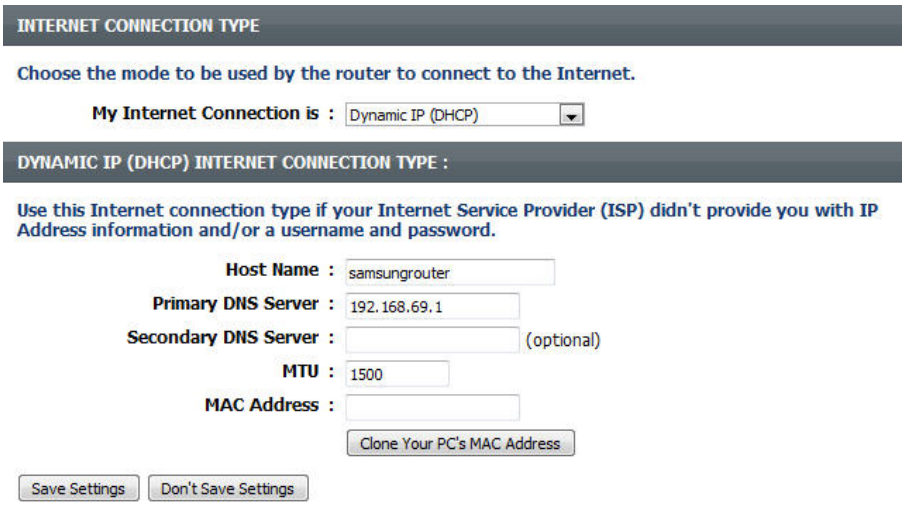
You can configure the following parameters:

IP Address:	Enter the Static IP address provided by the ISP here.
Subnet Mask:	Enter the Subnet Mask provided by the ISP here.
Gateway Address:	Enter the Gateway IP address provided by the ISP here.
Primary DNS Address:	Enter the Primary DNS IP address here.
Secondary DNS Address:	Enter the Secondary DNS IP address here. This field is normally optional. Only one DNS address is required for a functional Internet connection, but using a second DNS address provides more stability.
MTU:	Maximum Transmission Unit. You may need to change the MTU for optimal performance with your specific ISP. 1500 is the default MTU.
MAC Address:	The default MAC Address is set to the Internet port's physical interface MAC address on the Broadband Router. We recommend you leave it unchanged unless your are required to change it by your ISP. You can use the **Clone Your PC's MAC Address** button to replace the Internet port's MAC address with the MAC address of your Ethernet card.

Click the **Save Settings** button to accept the changes.
Click the **Don't Save Settings** button to discard the changes.

Internet Connection Type: Dynamic IP (DHCP)

If your IP uses Dynamic Addresses and provides IP addresses directly to your computer or other devices, select Dynamic IP (DHCP) from the drop-down menu to obtain IP Address information automatically. DHCP option is commonly used for cable modem services.



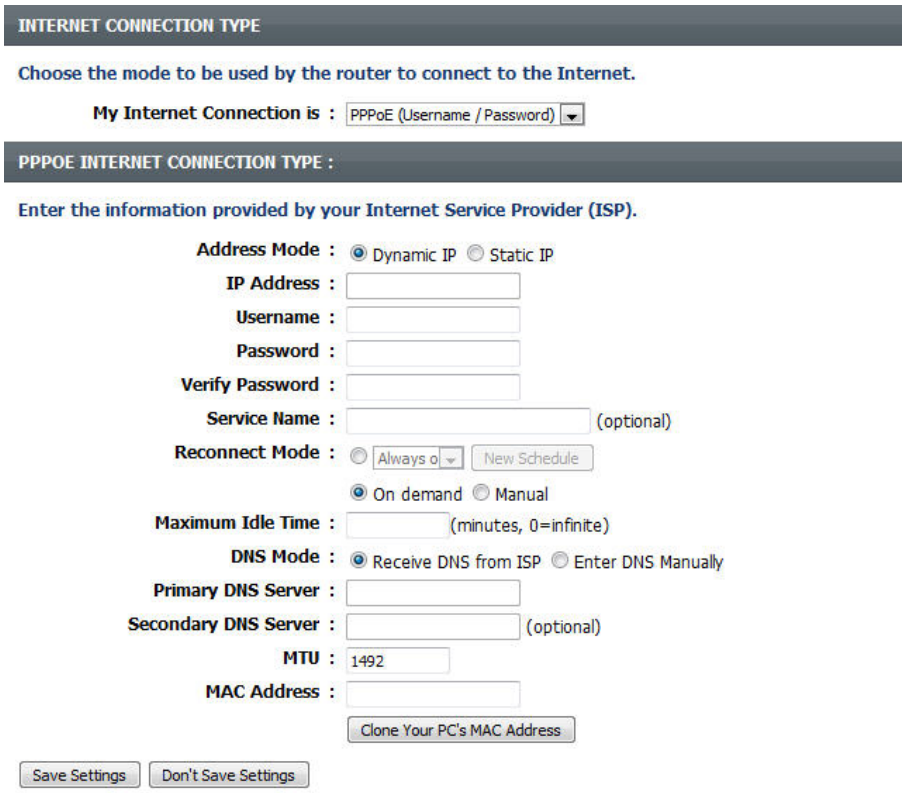
You can configure the following parameters:

Host Name:	The Host Name is optional, but may be required by some ISPs. Leave blank if you are not sure.
Primary DNS Server:	Enter the Primary DNS IP address here.
Secondary DNS Server:	Enter the Secondary DNS IP address here. This field is normally optional. Only one DNS address is required for a functional Internet connection, but using a second DNS address provides more stability.
MTU:	Maximum Transmission Unit. You may need to change the MTU for optimal performance with your specific ISP. 1500 is the default MTU.
MAC Address:	The default MAC Address is set to the Internet port's physical interface MAC address on the Broadband Router. We recommend you leave it unchanged unless your are required to change it by your ISP. You can use the **Clone Your PC's MAC Address** button to replace the Internet port's MAC address with the MAC address of your Ethernet card.

Click the **Save Settings** button to accept the changes.
Click the **Don't Save Settings** button to discard the changes.

Internet Connection Type: PPPoE (Username / Password)

Select PPPoE (Username/Password) from the drop-down menu if your ISP uses a PPPoE connection. Your ISP will provide you with a username and password. This option is typically used for DSL services. Make sure to remove your PPPoE software from your computer. The software is no longer needed and will not work through a router.



You can configure the following parameters. The list continues on the next page.

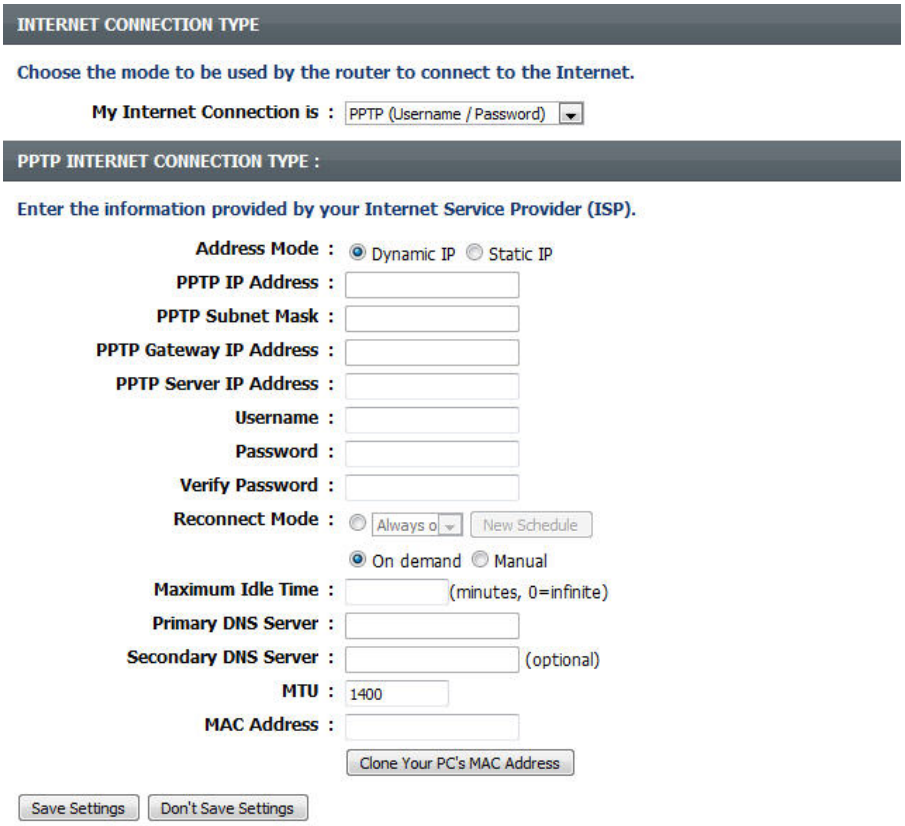
Address Mode:	Specify whether this Internet connection uses a Dynamic or Static IP address. PPPoE usually requires a Dynamic IP configuration.
IP Address:	If you selected Static IP, enter the PPPoE IP address here. This option is only available if Static IP is selected.
Username:	Enter the PPPoE account user name here. Get this information from the IP.
Password:	Enter the PPPoE account password used here. Get this information from the IP.
Verify Password:	Re-enter the PPPoE account password used here.
Service Name:	This optional field enables lets you enter a service name to identify this Internet connection.
Reconnect Mode:	Use the radio buttons to specify the reconnect mode. You can specify a custom schedule or specify the **On Demand** or **Manual** option. To specify a custom schedule, use the drop-down menu to select one of the schedules that has been defined in the Schedules page. To create a new schedule, click the **New Schedule** button to open the Schedules page. Schedules will be discussed later.
Maximum Idle Time:	Enter a maximum idle time during which the Internet connection is maintained during inactivity. To disable this feature, enable Auto-reconnect.

DNS Mode:	This option allows the router to obtain the DNS IP addresses from the ISP when you select **Receive DNS from ISP** or allows you to enter DNS IP address manually when you select **Enter DNS Manually**.
Primary DNS Server:	Enter the Primary DNS IP address here.
Secondary DNS Server:	Enter the Secondary DNS IP address here. This field is normally optional. Only one DNS address is required for a functional Internet connection, but using a second DNS address provides more stability.
MTU:	Maximum Transmission Unit. You may need to change the MTU for optimal performance with your specific ISP. 1492 is the default MTU.
MAC Address:	The default MAC Address is set to the Internet port's physical interface MAC address on the Broadband Router. We recommend you leave it unchanged unless your are required to change it by your ISP. You can use the **Clone Your PC's MAC Address** button to replace the Internet port's MAC address with the MAC address of your Ethernet card.

Click the **Save Settings** button to accept the changes.
Click the **Don't Save Settings** button to discard the changes.

Internet Connection Type: PPTP (Username / Password)

Select PPTP (Point-to-Point Tunneling Protocol) from the drop-down menu if your ISP uses a PPTP connection. Your ISP will provide you with a username and password. This option is typically used for DSL. services.



You can configure the following parameters. The list continues on the next page.

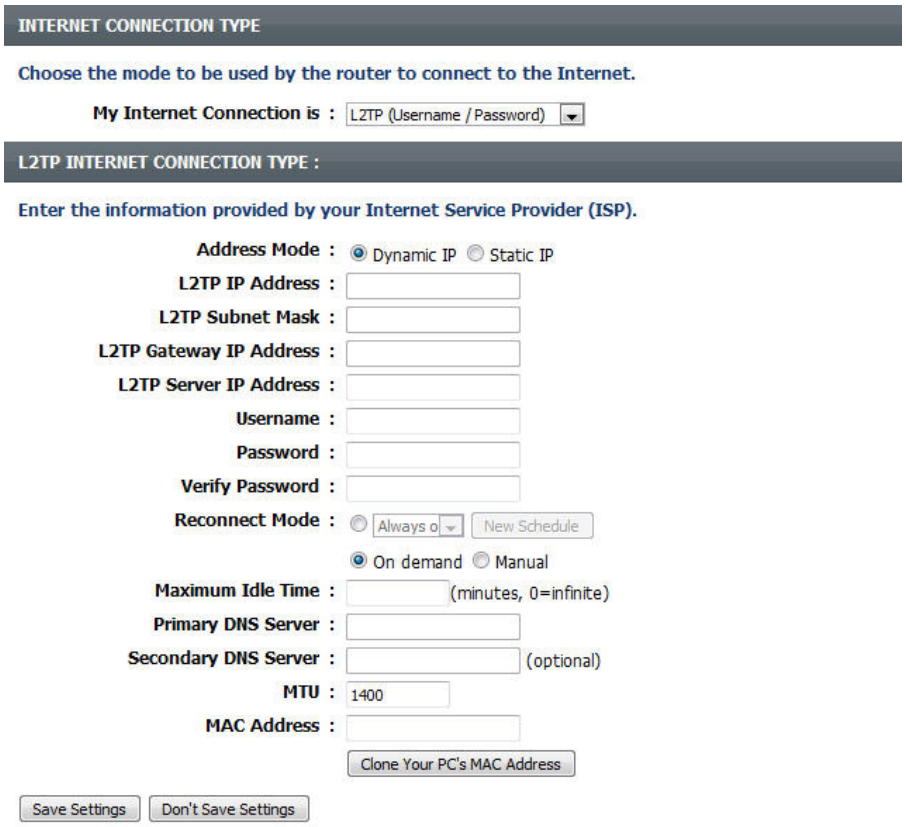
Address Mode:	Specify whether this Internet connection uses a Dynamic or Static IP address. PPTP usual requires a Dynamic IP configuration.
PPTP IP Address:	If you selected Static IP, enter the PPTP IP address here. This option is only available if you select Static IP.
PPTP Subnet Mask:	Enter the PPTP Subnet Mask here.
PPTP Gateway IP Address:	Enter the PPTP Gateway IP address here.
PPTP Server IP Address:	Enter the PPTP Server IP address here. This is normally the same a the PPTP Gateway IP address.
Username:	Enter the PPTP username here.
Password:	Enter the PPTP password here.
Verify Password:	Re-enter the PPTP password here.
Reconnect Mode:	Use the radio buttons to specify the reconnect mode. You can specify a custom schedule or specify the **On Demand** or **Manual** option. To specify a custom schedule, use the drop-down menu to select one of the schedules that has been defined in the Schedules page. To create a new schedule, click the **New Schedule** button to open the Schedules page. Schedules will be discussed later.

Maximum Idle Time:	Enter a maximum idle time during which the Internet connection is maintained during inactivity. To disable this feature, enable Auto-reconnect.
Primary DNS Server:	Enter the Primary DNS IP address here.
Secondary DNS Server:	Enter the Secondary DNS IP address here. This field is normally optional. Only one DNS address is required for a functional Internet connection, but using a second DNS address provides more stability.
MTU:	Maximum Transmission Unit. You may need to change the MTU for optimal performance with your specific ISP. 1400 is the default MTU.
MAC Address:	The default MAC Address is set to the Internet port's physical interface MAC address on the Broadband Router. We recommend you leave it unchanged unless your are required to change it by your ISP. You can use the **Clone Your PC's MAC Address** button to replace the Internet port's MAC address with the MAC address of your Ethernet card.

Click the **Save Settings** button to accept the changes.
Click the **Don't Save Settings** button to discard the changes.

Internet Connection Type: L2TP (Username / Password)

Choose L2TP (Layer 2 Tunneling Protocol) if your ISP uses a L2TP connection. Your ISP will provide you with a username and password. This option is typically used for DSL services.



You can configure the following parameters. The list continues on the next page.

Address Mode:	Specify whether this Internet connection uses a Dynamic or Static IP address. L2TP usual requires a Dynamic IP configuration.
L2TP IP Address:	If you selected Static IP, enter the L2TP IP address here. This option is only available if you selected Static IP.
L2TP Subnet Mask:	Enter the L2TP Subnet Mask address here.
L2TP Gateway IP Address:	Enter the L2TP Gateway IP address here.
L2TP Server IP Address:	Enter the L2TP Server IP address here. This is normally the same as the PPTP Gateway IP address.
Username:	Enter the L2TP username here.
Password:	Enter the L2TP password here.
Verify Password:	Re-enter the L2TP password here.
Reconnect Mode:	Use the radio buttons to specify the reconnect mode. You can specify a custom schedule or specify the **On Demand** or **Manual** option. To specify a custom schedule, use the drop-down menu to select one of the schedules that has been defined in the Schedules page. To create a new schedule, click the **New Schedule** button to open the Schedules page. Schedules will be discussed later.
Maximum Idle Time:	Enter a maximum idle time during which the Internet connection is maintained during inactivity. To disable this feature, enable Auto-reconnect.
Primary DNS Server:	Enter the Primary DNS IP address here.

Secondary DNS Server:	Enter the Secondary DNS IP address here. This field is normally optional. Only one DNS address is required for a functional Internet connection, but using a second DNS address provides more stability.
MTU:	Maximum Transmission Unit. You may need to change the MTU for optimal performance with your specific ISP. 1400 is the default MTU.
MAC Address:	The default MAC Address is set to the Internet port's physical interface MAC address on the Broadband Router. We recommend you leave it unchanged unless your are required to change it by your ISP. You can use the **Clone Your PC's MAC Address** button to replace the Internet port's MAC address with the MAC address of your Ethernet card.

Click the **Save Settings** button to accept the changes.
Click the **Don't Save Settings** button to discard the changes.

Wireless Settings

To access the Wireless Settings page, Click Wireless Settings on the left side of the Setup tab.

The Wireless Settings page provides 2 ways to configure the router's wireless settings:

- With the Wireless Network Setup Wizard
- Manually, for more experienced users

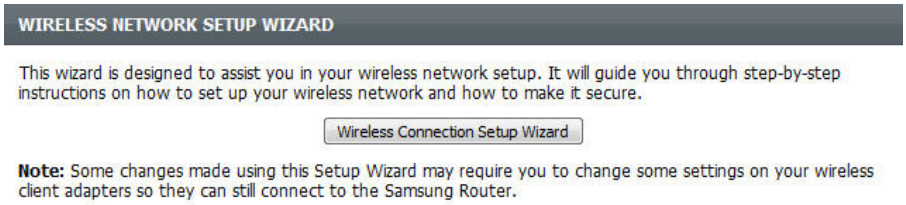
It also gives you access to the Wi-Fi Protected Setup (WPS) Wizard, which lets you connect WPS compliant wireless devices to your router literally at the touch of a button.

Configure your router first using the Wireless Network Setup Wizard. Then, if you have wireless devices that support the WPS connection method, use the Wi-Fi Protected Setup Wizard to connect them to the router. Wireless devices that support WPS usually have a labeled WPS (PBC) button. If you have wireless devices that are not WPS compliant, follow the directions that came with the device to connect to the router.

The Wireless Network Setup Wizard

The Wireless Network Setup Wizard is specially designed to provide basic network users with a simple, step-by-step set of instructions for configuring the wireless settings of this router.

To start the Wireless Network Setup Wizard, click the **Wireless Connection Setup Wizard** button.



The Welcome page appears.

Step 1: Enter a Custom Wireless Network Name

Enter a custom Wireless Network Name (also called an SSID) for each frequency band, 2.4GHz and 5Ghz, in the fields provided using up to 32 characters.

Step 2: Choose a Security Configuration

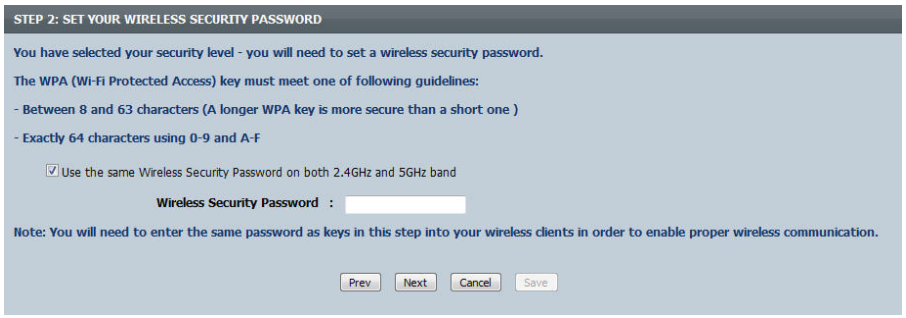
Select either '**Automatically assign a network key**' or '**Manually assign a network key**'. If you select '**Automatically assign a network key**' , the router automatically generates a WPA/WPA2 pre-shared key using the TKIP and AES encryption methods. If you select '**Manually assign a network key**', the router prompts you to enter a WPA2 pre-shared key manually using the TKIP and AES encryption methods. We strongly recommend using the automatic method to ensure your network is fully protected.

When done, click the **Next** button to continue. If you selected manual above, go to Step 3. If you selected automatic, go to Step 4.

You can also Click the **Prev** button to return to the previous page and Click the **Cancel** button to discard the changes and return to the main wireless page.

Step 3: Enter the Network Key Manually

If you chose to enter the Network Key manually, the screen below appears.



Manually enter the WPA/WPA2 pre-shared key in the **Wireless Security Password** space provided. If you want to use the same key for both frequency bands, select the '**Use the Same Wireless Security Password on both 2.4GHz and 5GHz band**' option. If not, leave the option unchecked and you can enter a different pre-shared key for each frequency band manually. The key you enter must be between 8 and 63 characters long.

You will have to enter this key into all wireless clients you want to connect to your network through this router that are not WPS compliant. We strongly recommend that you record this key.

Click the **Next** button to continue. The Setup Complete page appears.

Step 4: Complete the Setup

On the Setup Complete page, confirm that the configuration parameters are correct. Also, record the Pre-Shared key. You will have to enter the key into all wireless clients you want to connect to your network through this router that are not WPS compliant.

Click the **Save** button to accept the configuration. The router saves the settings and then re-displays the main Wireless Settings page.

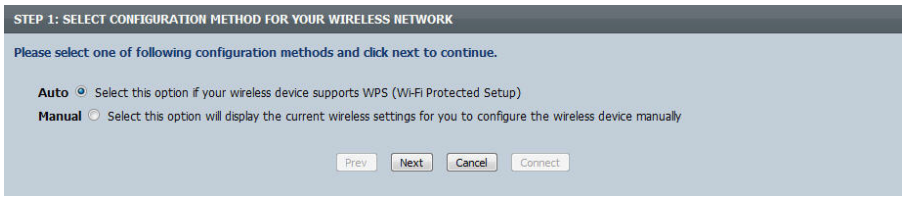
To connect WPS compliant devices to the router, go to the next page. To connect a Windows PC to the router wirelessly, go to "Connecting Your Computer to a Wireless Network" on page 98. To connect a Samsung TV to the router wirelessly, go to "Special Features of the CY-SWR1100" on page 92.

Wireless Settings: Wi-Fi Protected Setup Wizard

If a wireless client you want to connect to the router supports the WPS connection method, use the Wi-Fi Protected Setup Wizard to connect the device to the router. The Wi-Fi Protected Setup Wizard is specially designed to provide basic network users with a simple, step-by-step set of instructions to connect a wireless device to this router using the WPS method.

To start the Wi-Fi Protected Setup Wizard, click the **Add Wireless Device with WPS** button.

The Select Configuration Method page appears.

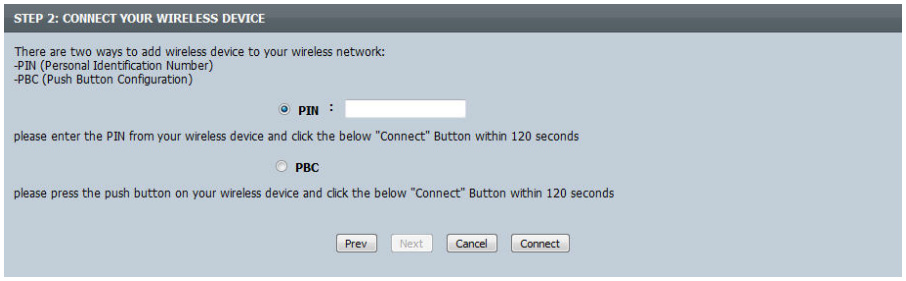


Step 1: Select the Configuration Method

On this page, select the Configuration Method. Choose **Auto** if your wireless client supports WPS or **Manual** if your wireless client does not support WPS.

When done, click the **Next** button to continue. If you selected Auto, the WPS Connect Your Wireless Device page appears. Go to Step 2. If you selected Manual, the Manual Connect Your Wireless Device page appears. Go to Step 4.

You can also Click the **Prev** button to return to the previous page or Click the **Cancel** button to return to the main wireless page.



Step 2: Select the WPS Connection Method

The WPS Connect Your Wireless Device page provides two ways to connect WPS compliant devices to the router: The **Personal Identification Number (PIN)** method and the Push Button Configuration method (PBC).

Select the PBC method if your device has a WPS(PBC) button. This will let you connect the device by pushing the WPS(PBC) button. Select the PIN method if your device does not have WPS(PBC) button or if you would prefer entering a PIN. If you select the PIN method, enter the PIN code of your device. The code should be on the device or in the device's documentation.

Step 3: Connect

Click the Connect button. If you selected the PBC method, click the WPS(PBC) button on the device within 120 seconds. When the device connects, the process is complete.

Step 4: Security Settings for Manual Connection

If you selected **Manual**, the router displays the Security Settings page. Record the settings you see here exactly. You will need to enter this information exactly as it appears on this page when you configure the connection settings for wireless clients that can't use the WPS method to connect.

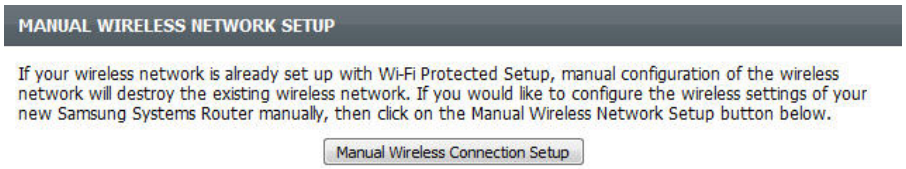
Click the **Prev** button to return to the previous page.

Click the **Cancel** button to return to the main wireless page.

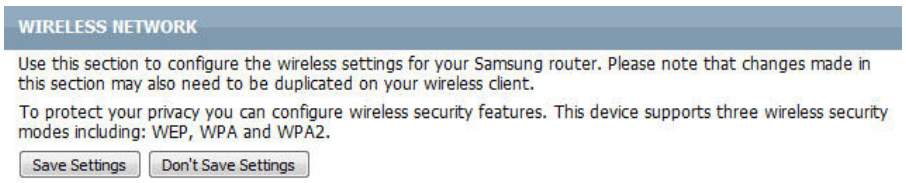
Click the **Wireless Status** button to navigate to the Status > Wireless page to see which wireless client are connected to the router.

Wireless Settings: Manual Wireless Network Setup

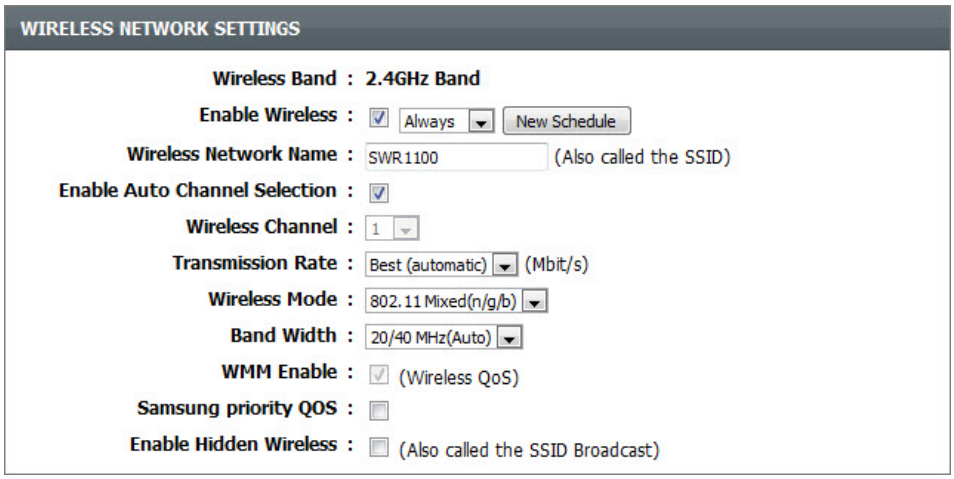
The manual wireless network setup option allows you to configure the wireless settings of this device manually. This option is for the more advanced users and includes all the parameters that can be configured for wireless connectivity.



To access the Manual Wireless Network Setup page, click the **Manual Wireless Connection Setup** button.



On this page, you can configure all the parameters related to the wireless connectivity of this router.



You can configure the following parameters. The list continues on the next page.

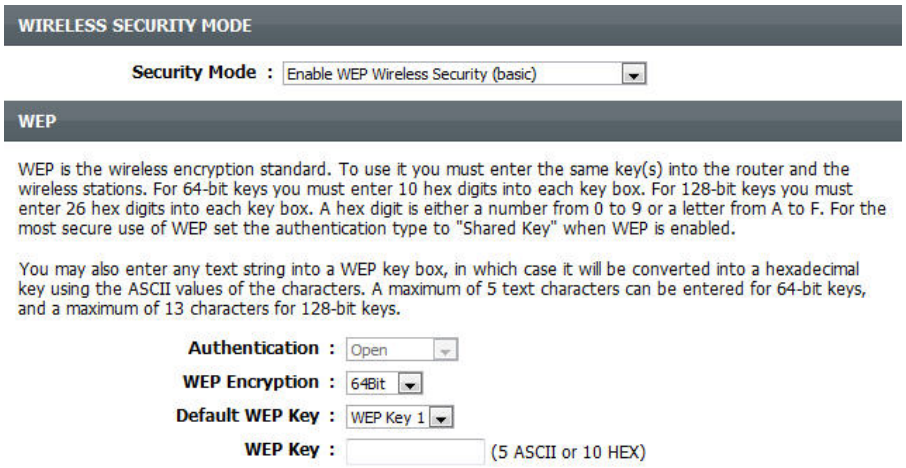
Wireless Band:	Displays the wireless band you are configuring. On this page, you are configuring the options for the 2.4GHz band.
Enable Wireless:	Check the box to enable the wireless function. If you do not want to use wireless, uncheck the box to disable all the wireless functions. Select the time frame that you would like your wireless network enabled. The schedule may be set to **Always**. Any schedule you create will be available in the drop-down menu. Click **New Schedule** to create a new schedule.
Wireless Network Name:	The Service Set Identifier (SSID) is the name of your wireless network. Create a name using up to 32 characters. The SSID is case-sensitive.
Enable Auto Channel Selection:	Check the box to let the router choose the channel with the least amount of interference automatically.
Wireless Channel:	By default the channel is set to 1. You can change the channel to match the channel of an existing wireless network or to customize the wireless network. If you enable Auto Channel Selection, this option will be greyed out.
Transmission Rate:	Select the transmission rate. We strongly recommend you select Best (Automatic) for best performance.
Wireless Mode:	Select the preferred frequency band to use for this wireless network.

Band Width:	When using the 802.11n frequency band, you can choose between a 20MHz or 20/40MHz bandwidth.
WMM Enable:	WMM (Wi-Fi Multimedia) is QoS for your wireless network. Check this box to improve the quality of video and voice applications for your wireless clients. This feature is not available in 802.11n configurations.
Samsung Priority QoS:	The Priority QoS function is unique to the CY-SWR1100. When you connect a Samsung TV to a Samsung wireless router using the 2.4GHz band, this function gives the Samsung TV a priority connection and ensures your TV gets the fastest throughput speed and displays the highest quality streaming contents. Check this box to use this function.
Enabled Hidden Wireless:	Check this box if you do not want the SSID of your wireless network to be broadcasted. If the SSID is hidden, the SSID will not be seen by Site Survey utilities, so your wireless clients will have to know the SSID of your router in order to connect to it.

By default, the wireless security of this router is disabled. In this next option, you can enabled or disable wireless security for the 2.4GHz band. There are two types of encryption you can use, WEP or WPA/WPA2.

Wireless Security Mode: WEP Wireless Security (basic)

Wired Equivalent Privacy (WEP) is the most basic form of encryption you can use for wireless networks. Even though it is known as a 'weak' security method, it is better than no security at all. Older wireless adapters sometimes only support WEP encryption. As a result, you can still find this encryption method used today.

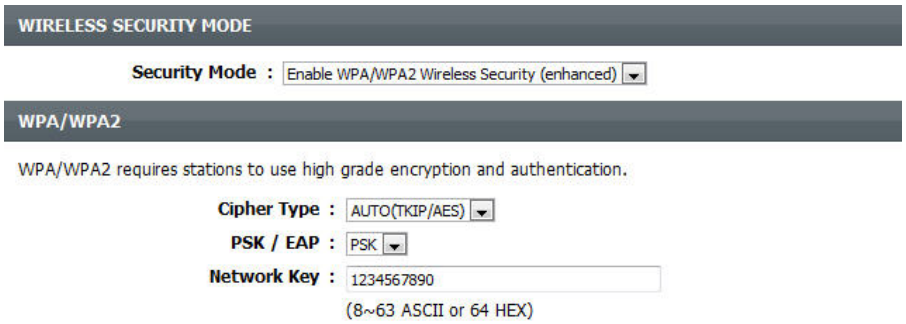


You can configure the following parameters:

Authentication:	Displays that the authentication method **Open System** is used.
WEP Encryption:	Specify use of a 64Bit or a 128Bit encrypted key.
Default WEP Key:	On some devices, you can have more than one WEP Key. On this router, you can only have one WEP Key. The Key number can only be set to 1.
WEP Key:	Enter the WEP key here. For 64-bit keys, you must enter 10 hex digits into the key entry field. For 128-bit keys, you must enter 26 hex digits into the key entry field. A hex digit is either a number from 0 to 9 or a letter from A to F. You can also enter a text string into the WEP key field and the router will convert the string into a hexadecimal key using the ASCII values of the characters. You can enter a maximum of 5 text characters for 64-bit keys and a maximum of 13 characters for 128-bit keys.

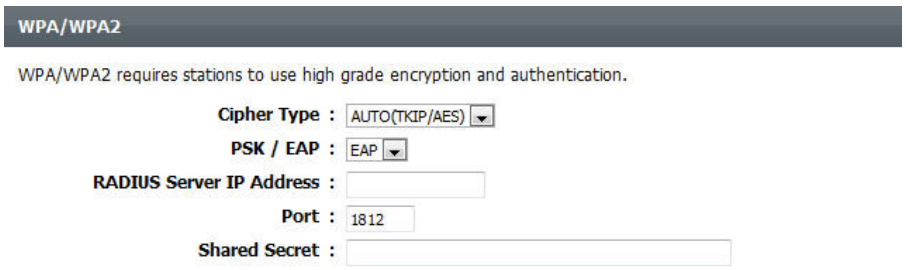
Wireless Security Mode: WPA/WPA2 Wireless Security (enhanced)

Wi-Fi Protected Access (WPA) is the most advanced and up to date wireless encryption method used today. This is the recommended wireless security option.

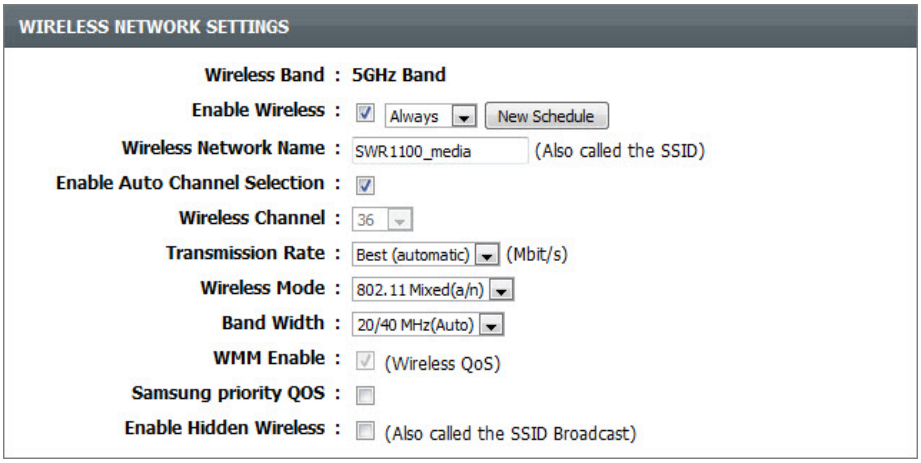


You can configure the following parameters:

Cipher Type:	Select the appropriate cipher type to use. The options are Temporal Key Integrity Protocol (**TKIP**), Advanced Encryption Standard (**AES**), and **Auto (TKIP/AES)**.
PSK/EAP:	WPA supports two authentication frameworks, Pre-Shared Key (PSK) and Extensible Authentication Protocol (EAP). PSK requires only the use of a pass-phrase (Shared Secret) for security. EAP, on the other hand, requires the installation of a RADIUS Server on the local network.
RADIUS Server IP Address:	If you choose the EAP authentication framework, enter the RADIUS server's IP address here.
Port:	If you choose the EAP authentication framework, enter the RADIUS server's port number here.
Shared Secret:	Enter the shared secret used here. This secret phrase needs to be the same on all of the wireless client for them to be able to connect to the wireless network successfully.



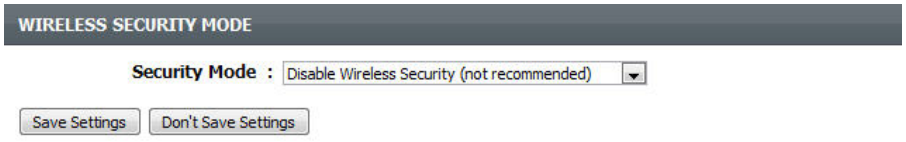
The next section lets you configure all the **5GHz** frequency band parameters.



You can configure the following parameters:

Wireless Band:	Displays the wireless band are configuring. On this page, you are configuring the options for the 5GHz band.
Enable Wireless:	Check the box to enable the wireless function. If you do not want to use wireless, uncheck the box to disable all the wireless functions. Select the time frame that you would like your wireless network enabled. The schedule may be set to **Always**. Any schedule you create will be available in the drop-down menu. Click **New Schedule** to create a new schedule.
Wireless Network Name:	The Service Set Identifier (SSID) is the name of your wireless network. Create a name using up to 32 characters. The SSID is case-sensitive.
Enable Auto Channel Selection:	Check the box to let the router choose the channel with the least amount of interference automatically.
Wireless Channel:	By default, the channel is set to 36. You can change the channel to match the channel of a an existing wireless network or to customize the wireless network. If you enable Auto Channel Selection, this option will be greyed out.
Transmission Rate:	Select the transmission rate. We strongly recommend you select Best (Automatic) for best performance.
Wireless Mode:	Select the preferred frequency band to use for this wireless network.
Band Width:	When using the 802.11n frequency band, you can choose between a 20MHz or 20/40MHz bandwidth.
WMM Enable:	WMM (Wi-Fi Multimedia) is QoS for your wireless network. Check this box to improve the quality of video and voice applications for your wireless clients. This feature is not available in 802.11n configurations.
Samsung Priority QoS:	The Priority QoS function is unique to the CY-SWR1100. When you connect a Samsung TV to a Samsung wireless router using the 5GHz band, this function gives the Samsung TV a priority connection and ensures your TV gets the fastest throughput speed and displays the highest quality streaming contents. Check this box to use this funtion.
Enabled Hidden Wireless:	Check this box if you do not want the SSID of your wireless network to be broadcast. If the SSID is hidden, the SSID will not be seen by Site Survey utilities, so your wireless clients will have to know the SSID of your router to connect to it.

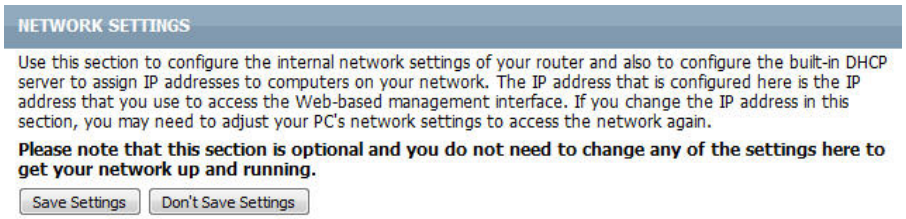
By default, the wireless security of this router is disabled. In this next option, you can enable or disable wireless security for the 5GHz band. These settings are identical to those we've discussed for the 2.4GHz security earlier.



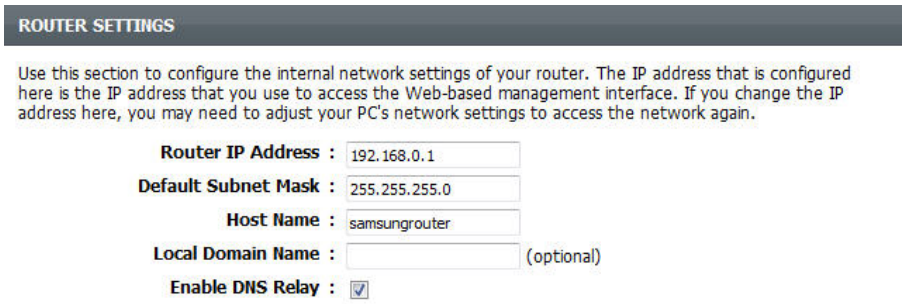
Click the **Save Settings** button to accept the changes.
Click the **Don't Save Settings** button to discard the changes.

Network Settings

On this page, you can configure the internal network settings of the router and configure the built-in DHCP server to assign IP addresses to computers on the network. The IP address you configure here is the IP address used to access the Web-based management interface. If you change the IP address in this section, you may need to adjust your PC's network settings to access the network again.



In the next section, you can configure the router settings of this device.



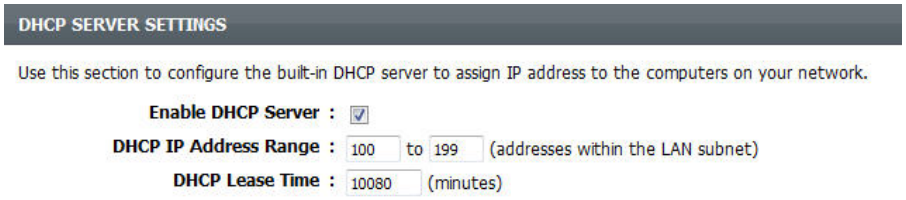
You can configure the following parameters:

Router IP Address:	Enter the IP address of the router. The default IP address is 192.168.0.1. If you change the IP address and you Click Apply, you will need to enter the new IP address in your browser to get back into the configuration utility.
Default Subnet Mask:	Enter the Subnet Mask. The default subnet mask is 255.255.255.0.
Host Name:	Enter a Host Name to identify this device.
Local Domain Name:	Enter the Domain name (Optional).
Enable DNS Relay:	Uncheck the box to transfer the DNS server information from your ISP to your computers. If checked, your computers will use the router for a DNS server.

DHCP Server Settings

DHCP stands for Dynamic Host Control Protocol. This device has a built-in DHCP server. The DHCP Server will automatically assign an IP address to the computers on the LAN/private network. Be sure to set your computers to be DHCP clients by setting their TCP/IP settings to "Obtain an IP Address Automatically." When you turn your computers on, they will automatically load the proper TCP/IP settings provided by the router. The DHCP Server will automatically allocate an unused IP address from the IP address pool to the requesting computer. You must specify the starting and ending address of the IP address pool.

At the bottom of the page, click the **Save Settings** button to accept the changes.
Click the **Don't Save Settings** button to discard the changes.



You can configure the following parameters:

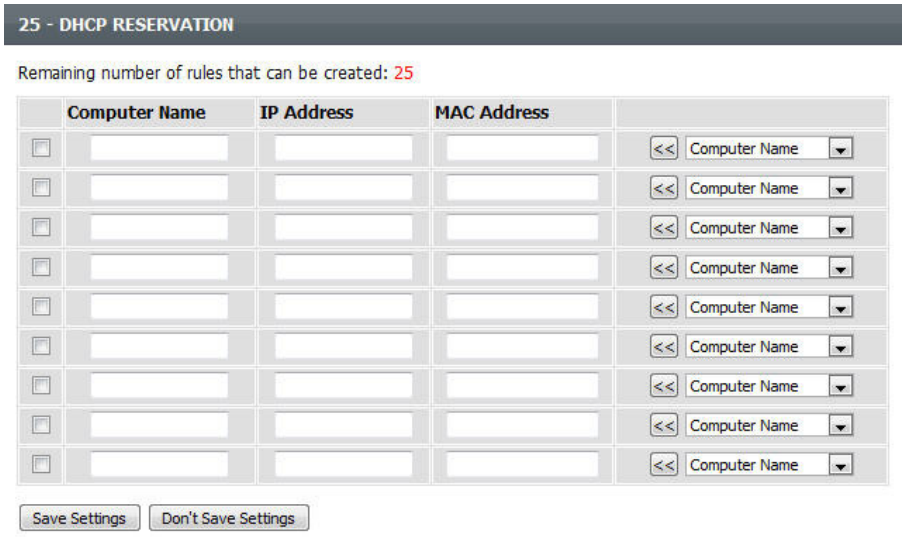
Enable DHCP Server:	Check this box to enable the DHCP server on your router. Uncheck to disable this function.
DHCP IP Address Range:	Enter the starting and ending IP addresses for the DHCP server's IP assignment.
DHCP Lease Time:	The length of time for the IP address lease. Enter the Lease time in minutes.

Note: If you statically (manually) assign IP addresses to your computers or devices, make sure the IP addresses are outside of this range or you may have an IP conflict.

The **DHCP Reservation List** displays a list of DHCP clients whose MAC address have been locked to specific IP addresses in the DHCP pool.

In the '**Number of Dynamic DHCP Clients**' section, all the active DHCP clients will be displayed.

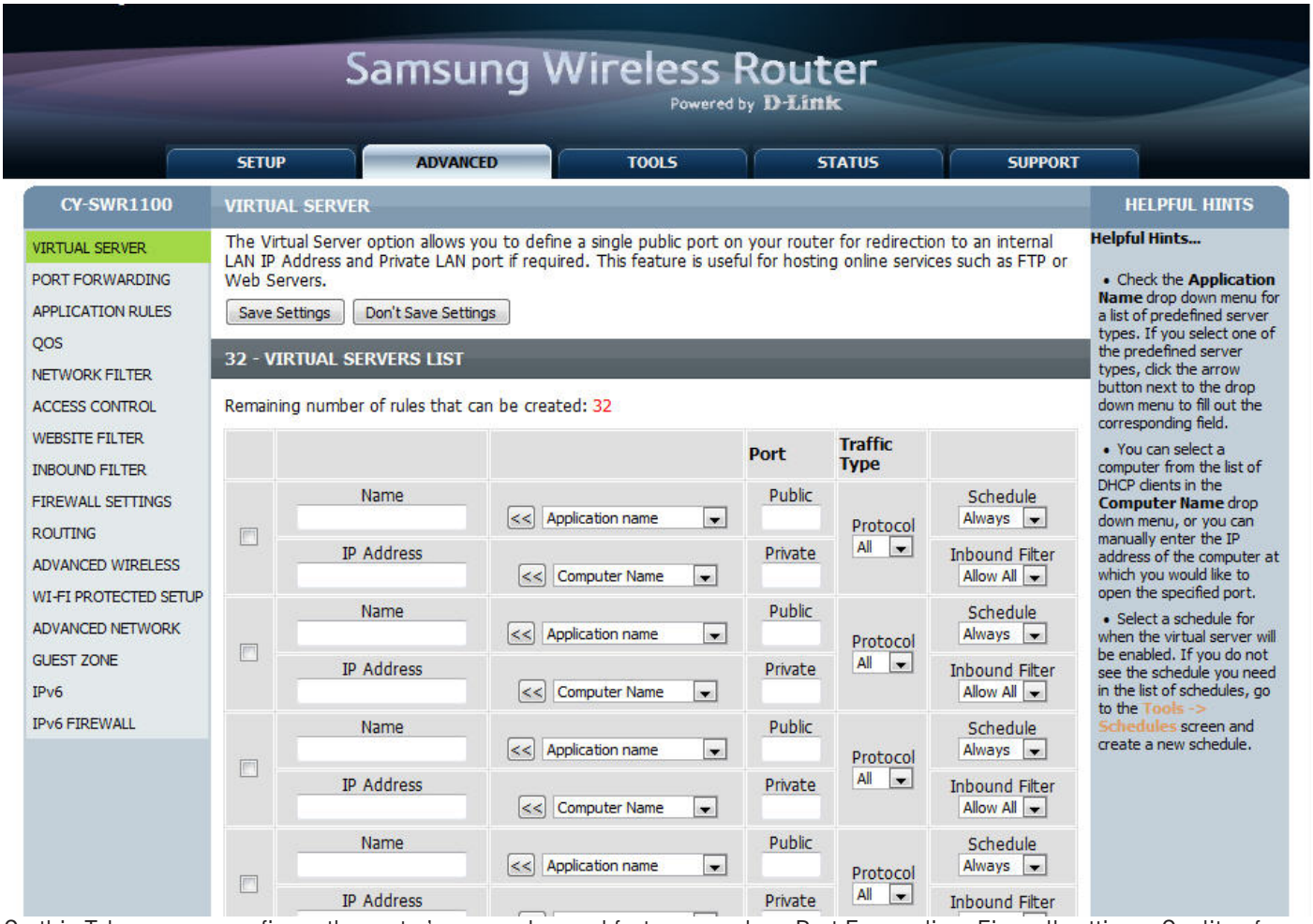
In the **DHCP Reservation** section, you can configure reserved IP address to selective DHCP clients by entering their MAC addresses in the list along with the appropriate IP address.



You can configure the following parameters:

Checkbox:	Check this box to enable the reservation.
Computer Name:	Enter the computer name. Alternatively, select a computer that currently has a DHCP lease from the drop down menu and Click << to automatically populate the Computer Name, IP Address, and MAC Address fields.
IP Address:	Enter the IP address you want to assign to the computer or device. This IP Address must be within the DHCP IP Address Range.
MAC Address:	Enter the MAC address of the computer or device.

ADVANCED TAB



On this Tab, you can configure the router's more advanced features, such as Port Forwarding, Firewall settings, Quality of Service settings and more.

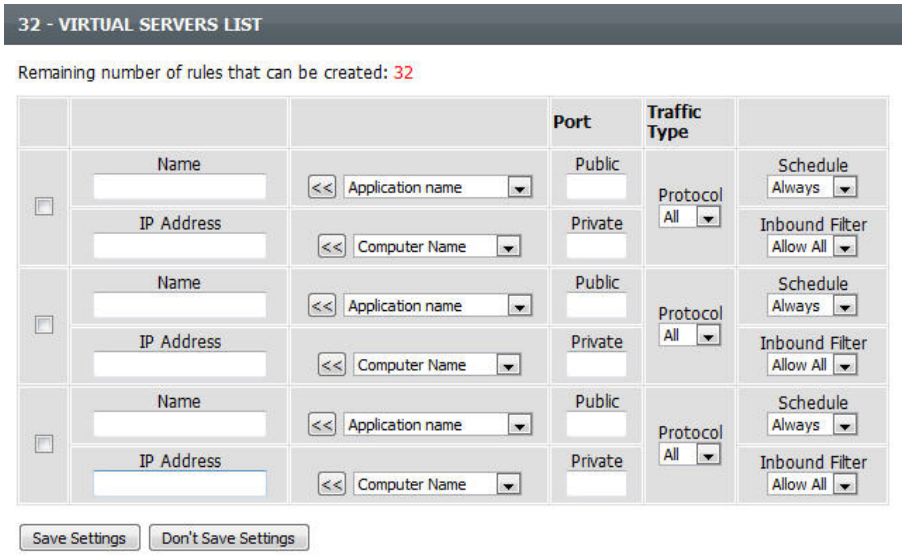
You can configure the following pages:

Virtual Server	On this page, you can configure Virtual Server policies related to this router.
Port Forwarding	On this page, you can forward a list of ports to an internal IP address.
Application Rules	On this page, you can create a set of application rules.
QoS	The QoS Engine option helps improve your network gaming performance by prioritizing applications. By default, the QoS Engine settings are disabled and application priority is not classified automatically.
Network Filter	On this page, you can configure network filtering rules.
Access Control	On this page, you can configure access control rules.
Website Filter	On this page, you can configure website and domain filtering rules.
Inbound Filter	On this page, you can configure Inbound Firewall Filtering rules.
Firewall Settings	On this page, you can configure some basic Firewall settings.
Routing	On this page, you can setup multiple routing profiles and rules.
Advanced Wireless	On this page, you can configure more advanced wireless properties.
Guest Zone	On this page, you can create and maintain guest zone for wireless access.
IPv6	On this page, you can configure the IPv6 connectivity of this device.
IPv6 Firewall	On this page, you can configure the IPv6 Firewall properties for this device.

Virtual Server

You can configure this router as a virtual server so that remote users accessing Web or FTP services via the public IP address can be automatically redirected to local servers in the LAN (Local Area Network). The router's firewall feature filters out unrecognized packets to protect the LAN network so all computers networked with the router are invisible to the outside world. You can make some of the LAN computers accessible from the Internet by enabling Virtual Server. Depending on the requested service, the router redirects the external service request to the appropriate server within the LAN network.
The router is also capable of port-redirection, meaning that incoming traffic to a particular port may be redirected to a different port on the server computer.

On this page, you can open external access to single ports.



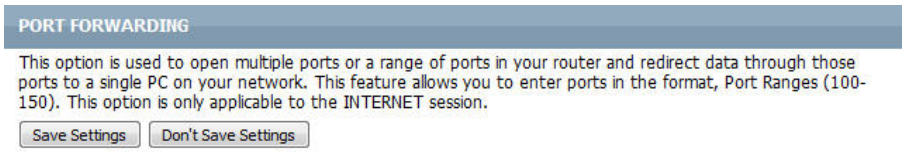
You can configure the following parameters:

Checkbox:	Check the box on the left side to enable the Virtual Server rule.
Name:	Enter a name for the rule or select an application from the drop-down menu. Select an application and Click << to populate the fields.
IP Address:	Enter the IP address of the computer on your local network that you want to allow the incoming service access to. If your computer is receiving an IP address automatically from the router (DHCP), you computer will be listed in the Computer Name drop-down menu. Select your computer and Click <<.
Port (Public/Private):	Enter the port that you want to open next to Public Port and Private Port. The public and private ports are usually the same. The public port is the port seen from the Internet side, and the private port is the port being used by the application on the computer within your local network.
Traffic Type:	Select TCP, UDP, or All from the Protocol drop-down menu.
Schedule:	Use the drop-down menu to schedule the time that the Virtual Server Rule will be enabled. The schedule may be set to Always, which will allow the particular service to always be enabled. You can create your own times in the Schedules page.

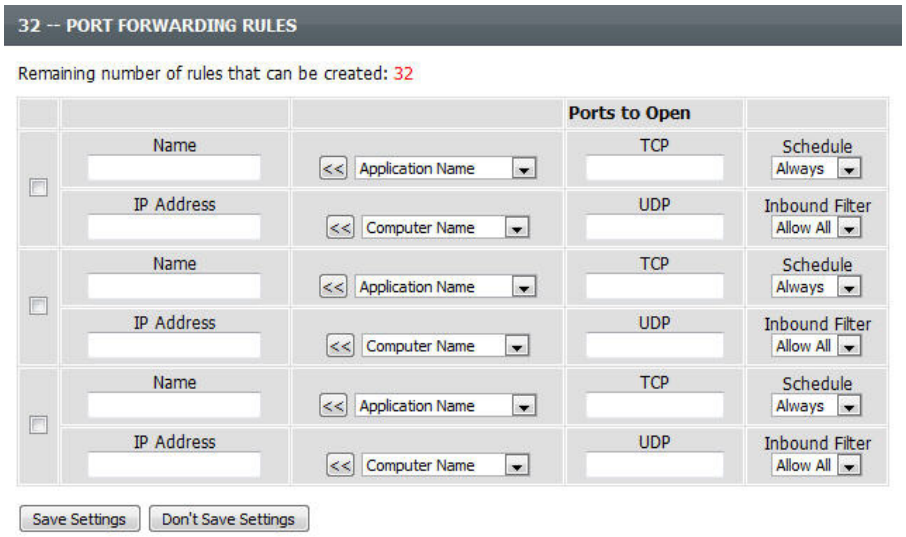
Click the **Save Settings** button to accept the changes.
Click the **Don't Save Settings** button to discard the changes.

Port Forwarding

On this page, you can forward a list of ports to an internal IP address.



The following section allows you to configure the port forwarding rules.



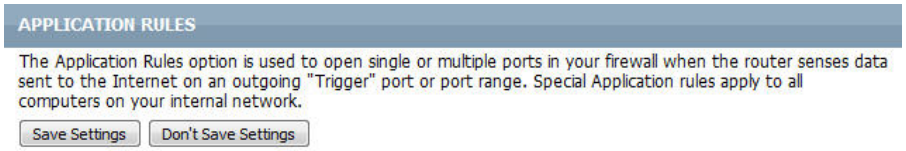
You can configure the following parameters:

Checkbox:	Check the box on the left side to enable the Port Forwarding rule.
Name:	Enter a name for the rule or select an application from the drop-down menu. Select an application and Click << to populate the fields.
IP Address:	Enter the IP address of the computer on your local network that you want to allow the incoming service access to. If your computer is receiving an IP address automatically from the router (DHCP), you computer will be listed in the Computer Name drop-down menu. Select your computer and Click <<.
Ports to Open (TCP/UDP):	Enter the external port number in the appropriate space provided. If the port number is TCP then enter the number in the TCP space, and if the port number is UDP than enter it in the UDP space.
Schedule:	Use the drop-down menu to schedule the time that the Port Forwarding rule will be enabled. The schedule may be set to Always, which will allow the particular service to always be enabled. You can create your own times in the Schedules page.
Inbound Filter:	Select the inbound filter rule here. Options to choose from are **Allow All**, **Deny All**, and any other custom rule you create.

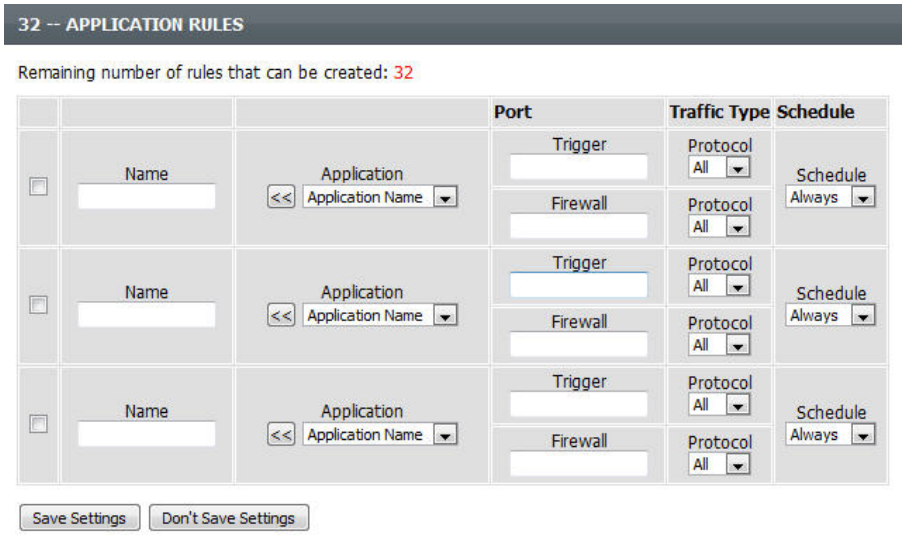
Click the **Save Settings** button to accept the changes.
Click the **Don't Save Settings** button to discard the changes.

Application Rules

Some applications, such as Internet gaming, video conferencing, Internet telephony and others, require muliple connections. These applications have difficulties working through NAT (Network Address Translation). Special Applications make some of these applications work with the router. If you need to run applications that require multiple connections, specify the port normally associated with an application in the “Trigger Port” field, select the protocol type as TCP or UDP, then enter the firewall (public) ports associated with the trigger port to open them for inbound traffic.



On this page, you can create a set of application rules.



You can configure the following parameters:

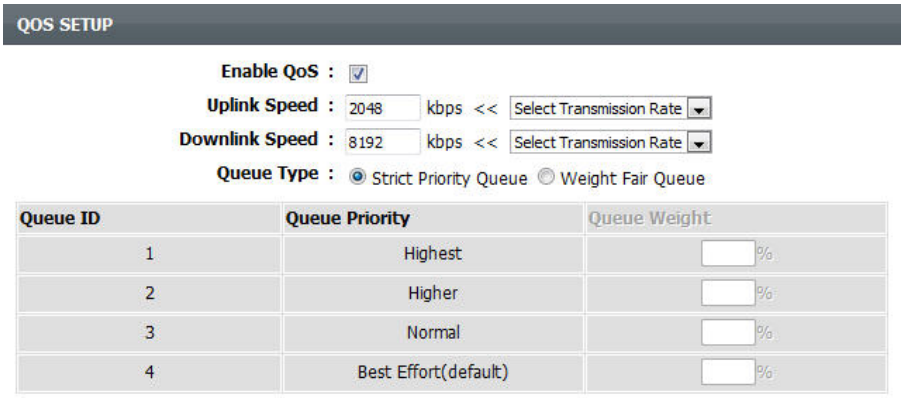
Checkbox:	Check the box on the left side to enable the Application Rule.
Name:	Enter a name for the rule. You may select a predefined application from the Application drop-down menu and Click <<.
Application:	Displays a list of predefined application to use in the rules.
Port (Trigger):	This is the port used to trigger the application. It can be either a single port or a range of ports.
Port (Firewall):	This is the port number on the Internet side that will be used to access the application. You may define a single port or a range of ports. You can use a comma to add multiple ports or port ranges.
Protocol:	Select the protocol of the firewall port (TCP, UDP, or All).
Schedule:	The schedule of times when the Application Rule will be enabled. The schedule may be set to Always, which will allow the particular service to always be enabled. You can create your own times in the Schedules page.

Click the **Save Settings** button to accept the changes.
Click the **Don’t Save Settings** button to discard the changes.

Quality of Service (QoS)

The QoS Engine option helps improve your network gaming performance by prioritizing applications. By default, the QoS Engine settings are disabled and application priority is not classified automatically.

Smart QoS improves VoIP voice quality or streaming by ensuring your VoIP or streaming traffic is prioritized over other network traffic, such as FTP or Web.

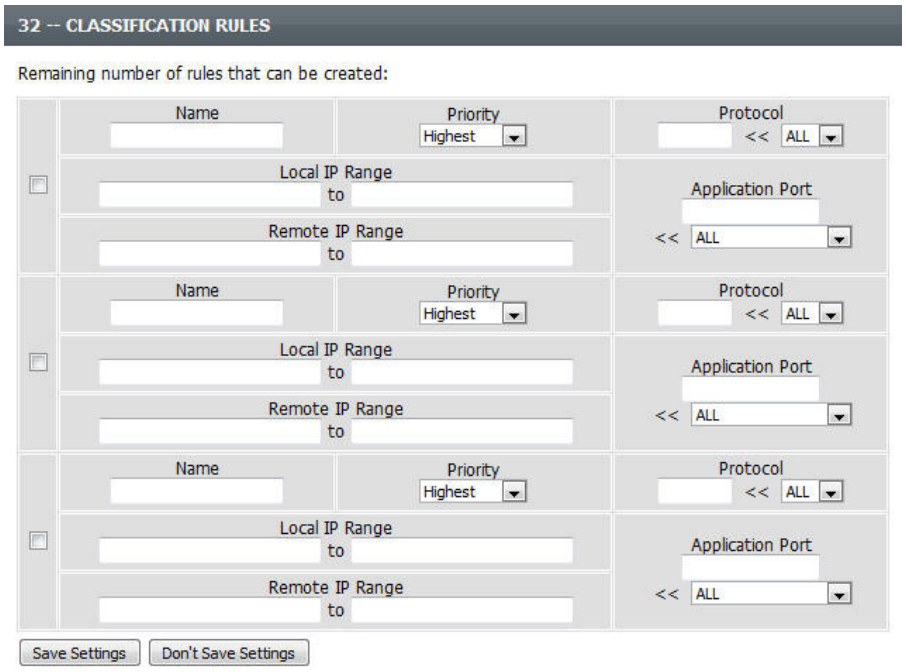


You can configure the following parameters:

Enable QoS:	This option is disabled by default. Enable this option for better performance and experience with online games and other interactive applications, such as VoIP.
Uplink Speed:	The speed at which data can be transferred from the router to your ISP. This is determined by your ISP. ISP's often define speed as a download/upload pair. For example, 1.5Mbits/284Kbits. Using this example, you would enter 284. Alternatively you can test your uplink speed with a service such as www.dslreports.com.
Downlink Speed:	The speed at which data can be transferred from the ISP to the router. This is determined by your ISP. ISP's often define speed as a download/upload pair. For example, 1.5Mbits/284Kbits. Using this example, you would enter 1500. Alternatively you can test your downlink speed with a service such as www.dslreports.com.
Queue Type:	Here You can specify the queue type used. When choosing the option **Strict Priority Queue**, the router will apply QoS based on the internal specification for the queue ID's listed. When choosing the option **Weight Fair Queue**, the router will apply QoS based on You defined percentage in the Queue Weight column.
Queue ID:	In this column the Queue ID used will be displayed.
Queue Priority:	In this column the Queue Priority used will be displayed.
Queue Weight:	After choosing to use the Weight Fair Queue option under Queue Type, you can enter the Queue Weight for each individual Queue ID.

Click the **Save Settings** button to accept the changes.
Click the **Don't Save Settings** button to discard the changes.

After specifying the QoS framework used in the QoS setup section, you can now create individual rules for scenarios that require the use of traffic control and data priority manipulation.



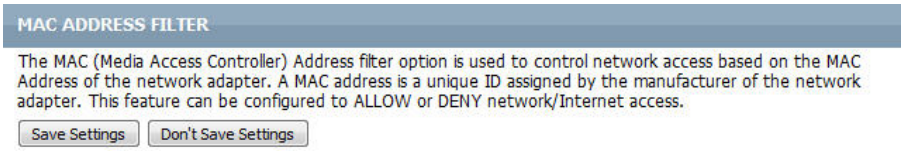
You can configure the following parameters:

Checkbox:	Check this option to enable the rule specified.
Name:	Enter a custom name for the rule being created here. This name is used for identification.
Priority:	Select the appropriate priority requirement from the drop-down menu. You can choose **Highest**, **Higher**, **Normal**, and **Best Effort**.
Protocol:	Select the protocol used for the application in the drop-down menu and it will automatically place it in the Protocol field.
Local IP Range:	Enter the local IP range here. This is the IP range of you Local Area Network. The Router's IP cannot be included in this range.
Remote IP Range:	Enter the remote IP range here. This is the IP range of the public network from the Internet Port side. To apply this rule to any IP addresses from the public side, enter the range 0.0.0.1 to 255.255.255.254.
Application Port:	Enter the application port number used here.

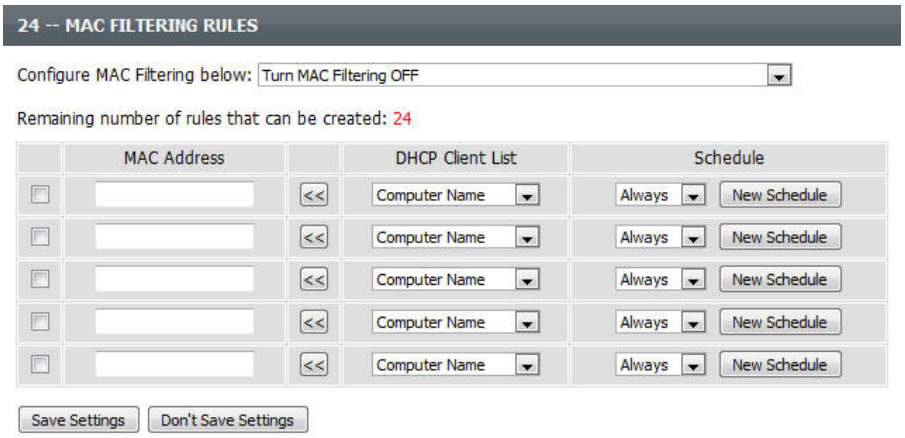
Click the **Save Settings** button to accept the changes.
Click the **Don't Save Settings** button to discard the changes.

Network Filter

The MAC (Media Access Controller) Address filter option is used to control network access based on the MAC Addresses of network adapters (network access cards, etc.) A MAC address is a unique ID assigned by the manufacturer to each network adapter. You can configure this feature to ALLOW or DENY network/Internet access.



In the **MAC Filtering Rules** section, you can create and edit Network filter rules. This maximum number of rules you can create is 24.



You can configure the following parameters:

Configure MAC Filtering:	From the drop down list, you can select Turn MAC Filtering OFF, Turn MAC Filtering ON and ALLOW computers listed to access the network, or Turn MAC Filtering ON and DENY computers listed to access the network .
Checkbox:	Check the box on the left side to enable the Network Filter.
MAC Address:	Enter the MAC address you would like to use in this filtering rule.
DHCP Client List:	Select a DHCP client from the Computer Name drop-down menu and Click << to copy that MAC Address.
Schedule:	The schedule of times when the Network Filter will be enabled. The schedule may be set to Always, which will allow the particular service to always be enabled. Click the New Schedule button to create your own times in the Schedules page.

Click the **Save Settings** button to accept the changes.
Click the **Don't Save Settings** button to discard the changes.

Access Control

The Access Control option allows you to control access in and out of your network. Use this feature to only grant access to approved sites, limit web access based on time or dates, and/or block internet access for applications like P2P utilities or games.

In the **Access Control** section, you can enable the access control feature and add new access control policies.

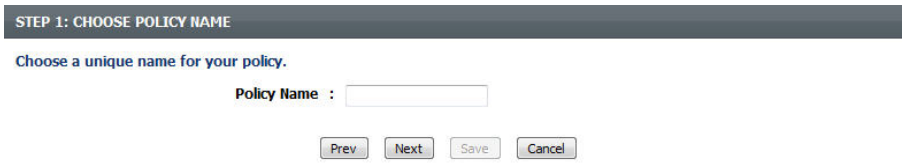
You can configure the following parameters:

Enable Access Control:	Check this option to enable the Access Control feature.
Add Policy:	Click this button to add a new Access Control Policy.

After you Click the **Add Policy** button, the add policy wizard will guide you step-by-step through process of adding a new policy. The first window explains the process.

Click the **Next** button to continue to the next window.
Click the **Cancel** button to discard the changes made and return to the main Access Control window.

Step 1: Enter the policy name.

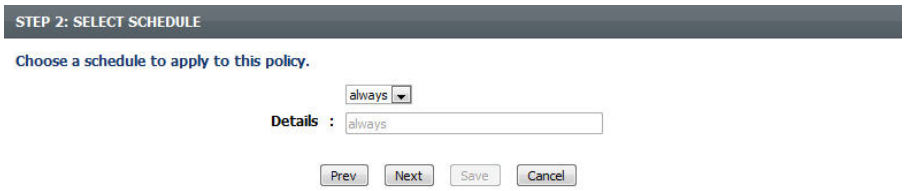


You can configure the following parameters:

Policy Name:	Enter the new policy name for this rule here.

Click the **Prev** button to return to the previous window.
Click the **Next** button to continue to the next window.
Click the **Cancel** button to discard the changes made and return to the main Access Control window.

Step 2: Configure the schedule settings for this rule.

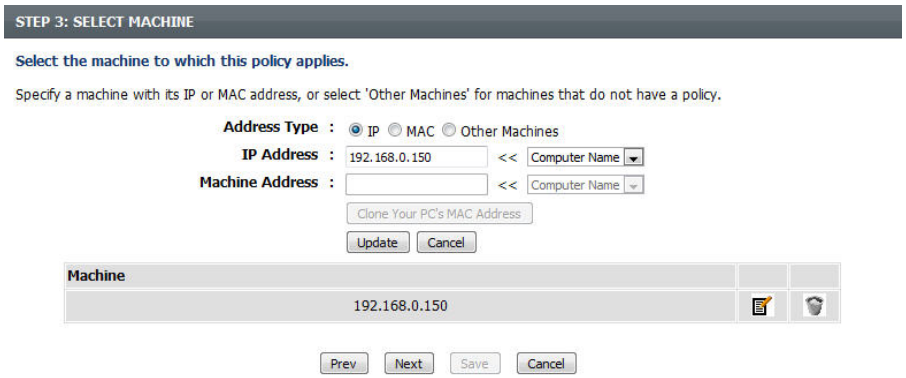


You can configure the following parameters:

Details:	Select the appropriate predefined schedule rule to apply to this rule from the drop-down menu.

Click the **Prev** button to return to the previous window.
Click the **Next** button to continue to the next window.
Click the **Cancel** button to discard the changes made and return to the main Access Control window.

Step 3: Configure the address type and IP address of the machines used in this rule.

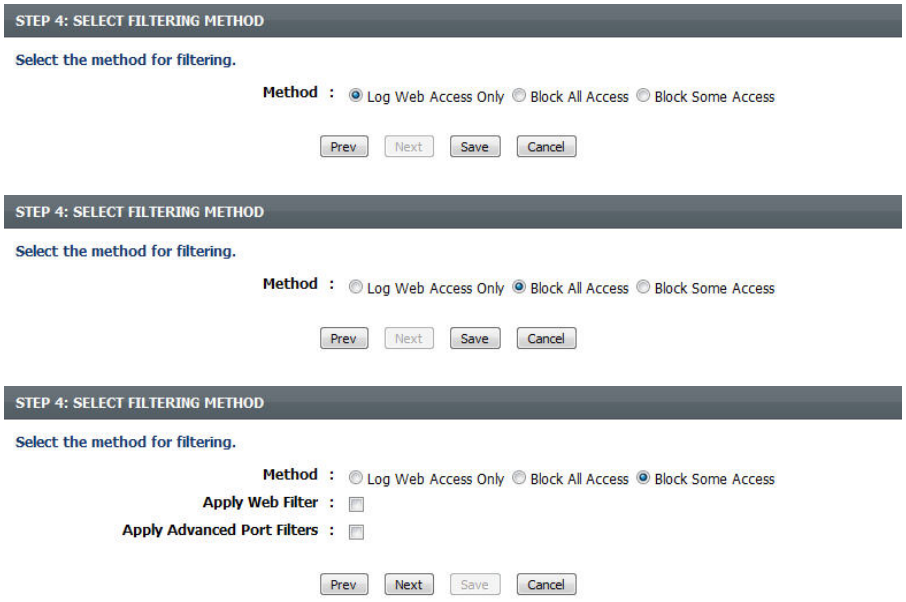


You can configure the following parameters:

Address Type:	Specify a machine with its IP or MAC address, or select 'Other Machines' for machines that do not have a policy.
IP Address:	After selecting the IP address type, you can enter the IP address of the machines used in this rule here. Alternatively, you can select a Computer from the **Computer Name** list.
Machine Address:	After selecting the MAC address type, you can enter the MAC address of the machine used in this rule here. Alternatively, you can select a Computer from the **Computer Name** list.
Add:	Click this button to add the machine to the list.
Update:	After Clicking the option, you can to update the machine information.
Delete:	To remove a machine from the list, click the icon.

Click the **Prev** button to return to the previous window.
Click the **Next** button to continue to the next window.
Click the **Cancel** button to discard the changes made and return to the main Access Control window.

Step 4: Select the filtering method used for this rule.

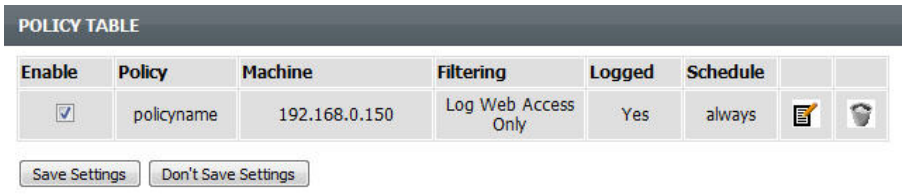


You can configure the following parameters:

Method:	Select the filtering method. Choose from '**Log Web Access Only**', '**Block All Access**', and '**Block Some Access**'.
Apply Web Filter:	If you select the '**Block Some Access**' option, this option becomes accessible. Selecting this option allows the web filter access control feature to be applied to this rule.
Apply Advance Port Filters:	If you select the '**Block Some Access**' option, this option becomes accessible. Selecting this option allows the advanced port filters access control feature to be applied to this rule.

Click the **Prev** button to return to the previous window.
Click the **Next** button to continue to the next window.
Click the **Cancel** button to discard the changes made and return to the main Access Control window.
Click the **Save** button to accept the changes made and return to the main Access Control window.

In the Policy Table section, a list of access control rules is displayed. To edit a specific rule, click the icon. To remove a specific rule, click the icon.



Click the **Save Settings** button to accept the changes.
Click the **Don't Save Settings** button to discard the changes.

Website Filter

Website Filters allow you to set up a list of Web sites that can be viewed by multiple users through the network.

Website Filters allows or denies computers on your network access to specific web sites by keywords or specific Domain Names. Select '**ALLOW computers access to ONLY these sites**' to allow computers on your network to access only specified URLs and Domain Names. Select '**DENY computers access to ONLY these sites**' to deny computers on your network access to specified URLs and Domain Names.

You can configure the following parameters:

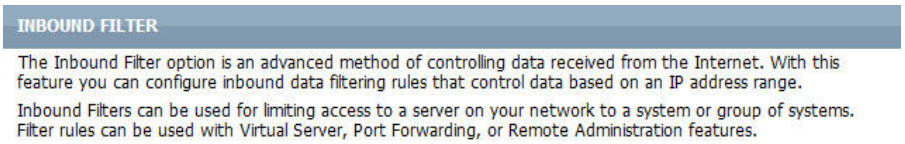
Website URL/Domain:	Enter the URL or Domain name that you want to allow or block here. An example of an URL is: http://www.facebook.com/ An example of a domain name is: facebook.com

Click the **Clear the list below...** button to remove all the entries from the spaces in the list.

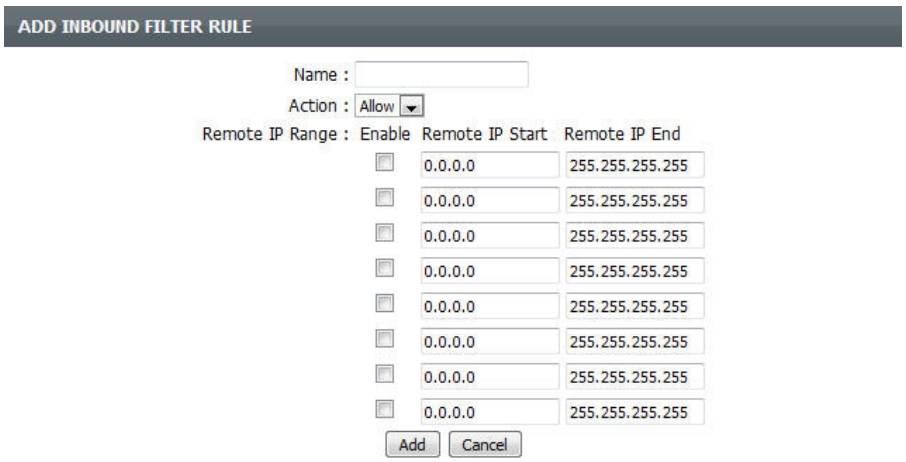
Click the **Save Settings** button to accept the changes.
Click the **Don't Save Settings** button to discard the changes.

Inbound Filter

The Inbound Filter option is an advanced method of controlling data received from the Internet. With this feature you can configure inbound data filtering rules that control data based on an IP address range.



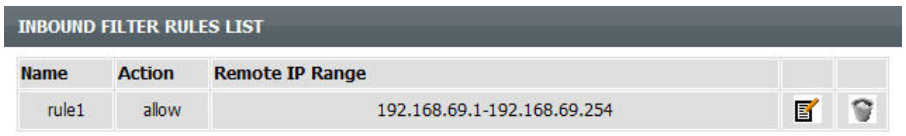
Inbound Filters can be used for limiting access to a server on your network to a system or group of systems. Filter rules can be used with Virtual Server, Port Forwarding, or Remote Administration features. You can add new Inbound filter rule in the next section.



You can configure the following parameters:

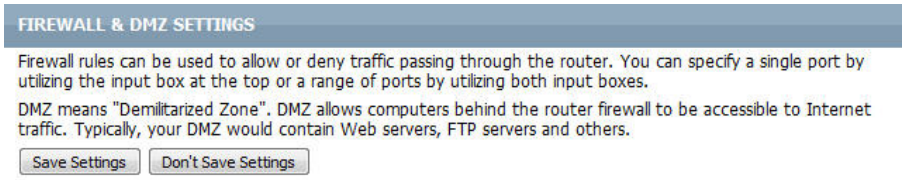
Name:	You can enter a custom name for the inbound filter rule here.
Action:	Select an action that will take place when this rule is initiated. Choose **Allow** and **Deny**.
Enable:	Check this option to enable the specified IP range for this rule.
Remote IP Start:	Enter the remote starting IP address in the range here.
Remote IP End:	Enter the remote ending IP address in the range here.
Add:	Click this button to add the new inbound filter rule.
Cancel:	Click this button to discard the new inbound filter rule.

In the **Inbound Filter List** section, you can view a list of the inbound filter rules already created. To edit a specific rule, click the appropriate icon. The delete a specific rule, click the icon.



Firewall Settings

A firewall protects your network from the outside world. The router offers a firewall type functionality. The SPI feature helps prevent cyber attacks. Sometimes you may want a computer exposed to the outside world for certain types of applications. If you choose to expose a computer, you can enable DMZ. DMZ is short for Demilitarized Zone. This option will expose the chosen computer completely to the outside world.



You can use Firewall rules to allow or deny traffic passage through the router. You can specify a single port by utilizing the input box at the top or a range of ports by utilizing both input boxes. DMZ means “Demilitarized Zone”. DMZ allows computers behind the router firewall to be accessible to Internet traffic. Typically, your DMZ would contain Web servers, FTP servers and others.

You can configure the following parameters:

Enable SPI:	Check the Enable SPI box to enable the SPI (Stateful Packet Inspection, also known as dynamic packet filtering) feature. Enabling SPI helps to prevent cyber attacks by tracking more states per session. It validates that the traffic passing through the session conforms to the protocol.

In the **DMZ Host** section, you can configure the DMZ settings for this router.

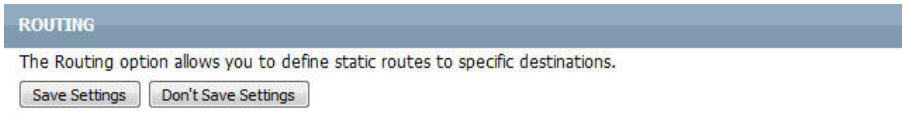
You can configure the following parameters:

Enable DMZ:	Check this option to enable the DMZ feature.
DMZ IP Address:	Enter the IP address of the computer on the LAN that you want to have unrestricted Internet communication into the DMZ IP address field. To specify an existing DHCP client, use the Computer Name drop-down to select the computer that you want to make a DMZ host. If selecting a computer that is a DHCP client, be sure to make a static reservation in the Setup > Network Settings page so that the IP address of the DMZ machine does not change.

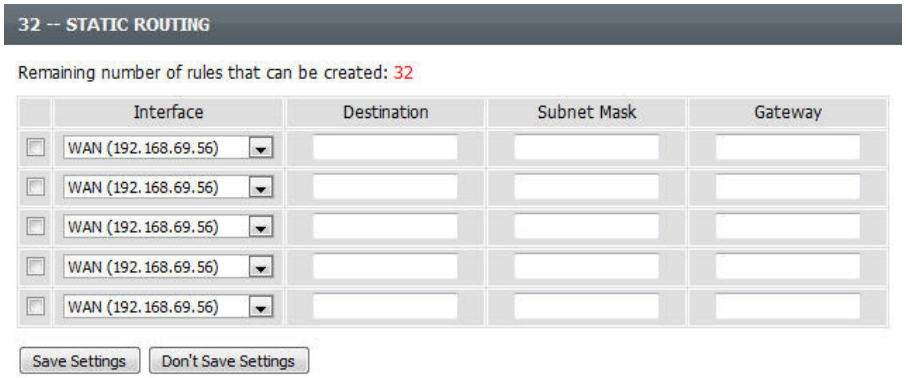
Click the **Save Settings** button to accept the changes.
Click the **Don’t Save Settings** button to discard the changes.

Routing

The Routing option is an advanced method of customizing specific routes of data through your network.



In the **Static Routing** section, You can configure routing rules used by this router. The maximum number of rules that can be configured is 32.



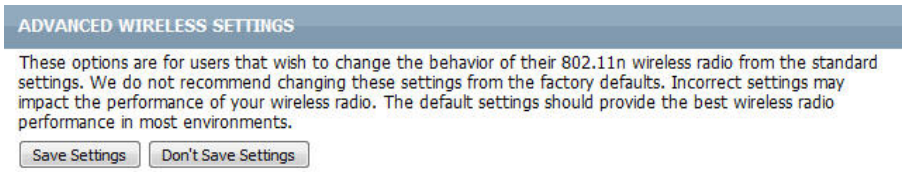
You can configure the following parameters:

Checkbox:	To enable a route, check the box that is on the left side of the route.
Interface:	Use the drop-down menu to specify if the IP packet must use the WAN or LAN interface to transit out of the Router.
Destination:	Enter the IP address of the packets that will take this route.
Subnet Mask:	Enter the subnet mask to specify the subnet of the IP packets that will take this route.
Gateway:	Enter the next hop that will be taken if this route is used.

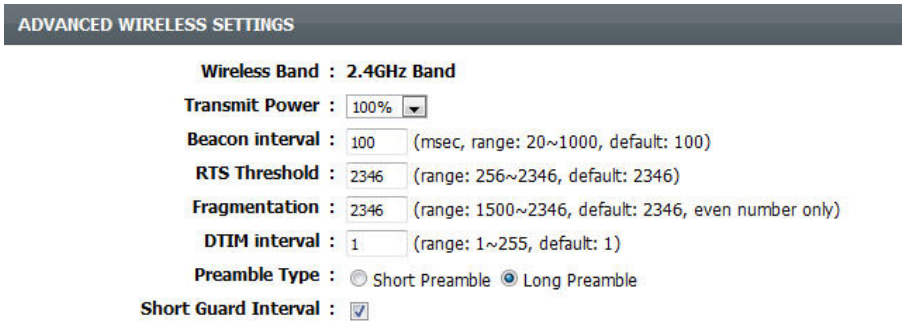
Click the **Save Settings** button to accept the changes.
Click the **Don't Save Settings** button to discard the changes.

Advanced Wireless

These options are for users that wish to change the behavior of their 802.11n wireless radio from the standard settings. We do not recommend changing these settings from the factory defaults. Incorrect settings may impact the performance of your wireless radio. The default settings should provide the best wireless radio performance in most environments.



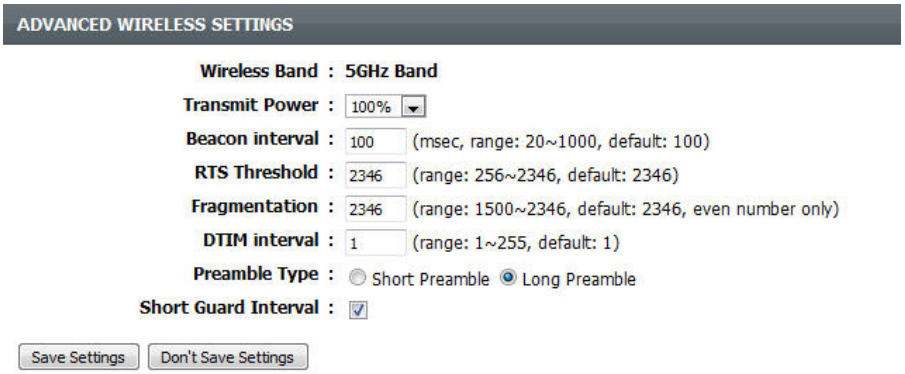
In the next section, You can configure the more advanced wireless settings for the **2.4GHz frequency** band.



You can configure the following parameters:

Wireless Band:	You can view the wireless frequency band you are configuring - in the case, the 2.4GHz band.
Transmit Power:	This option sets the transmit power of the antennas.
Beacon Interval:	Beacons are packets sent by an Access Point to synchronize a wireless network. Specify a value. 100 is the default setting and is recommended.
RTS Threshold:	You can enter the RTS threshold value used. This value should remain at its default setting of 2346. If inconsistent data flow is a problem, only a minor modification should be made.
Fragmentation:	The fragmentation threshold, which is specified in bytes, determines whether packets will be fragmented. Packets exceeding the 2346 byte setting will be fragmented before transmission. 2346 is the default setting.
DTIM Interval:	You can enter the DTIM Interval value. Delivery Traffic Indication Message (DTIM) is a count-down informing clients of the next window for listening to broadcast and multicast messages. The default settings is 1.
Preamble Type:	Use the radio buttons to specify whether the Router should use the **Short Preamble** or **Long Preamble** type. The preamble type defines the length of the CRC (Cyclic Redundancy Check) block for communication between the Router and roaming wireless adapters.
Short Guard Interval:	Check this box to reduce the guard interval time therefore increasing the data capacity. However, it's less reliable and may create higher data loss.

In the next section, you can configure the more advanced wireless settings for the **5GHz frequency** band.



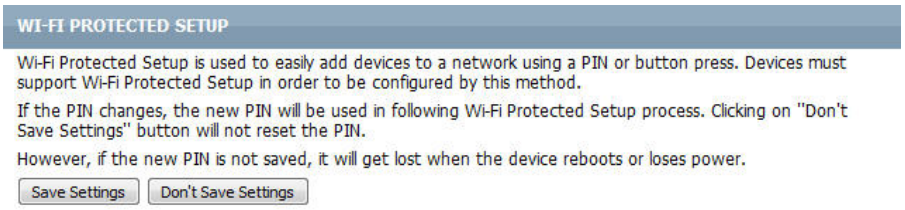
You can configure the following parameters:

Wireless Band:	You can view the wireless frequency band you are configuring - in the case, the 5GHz band.
Transmit Power:	This option sets the transmit power of the antennas.
Beacon Interval:	Beacons are packets sent by an Access Point to synchronize a wireless network. Specify a value. 100 is the default setting and is recommended.
RTS Threshold:	You can enter the RTS threshold value used. This value should remain at its default setting of 2346. If inconsistent data flow is a problem, only a minor modification should be made.
Fragmentation:	The fragmentation threshold, which is specified in bytes, determines whether packets will be fragmented. Packets exceeding the 2346 byte setting will be fragmented before transmission. 2346 is the default setting.
DTIM Interval:	You can enter the DTIM Interval value. Delivery Traffic Indication Message (DTIM) is a count-down informing clients of the next window for listening to broadcast and multicast messages. The default settings is 1.
Preamble Type:	Use the radio buttons to specify whether the Router should use the **Short Preamble** or **Long Preamble** type. The preamble type defines the length of the CRC (Cyclic Redundancy Check) block for communication between the Router and roaming wireless adapters.
Short Guard Interval:	Check this box to reduce the guard interval time therefore increasing the data capacity. However, it's less reliable and may create higher data loss.

Click the **Save Settings** button to accept the changes.
Click the **Don't Save Settings** button to discard the changes.

Wi-Fi Protected Setup

Wi-Fi Protected Setup (WPS) System is a simplified method for securing your wireless network during the "Initial setup" as well as the "Add New Device" processes. The Wi-Fi Alliance (WFA) has certified it across different products as well as manufactures. The process is as easy as depressing a button for the Push-Button Method or correctly entering the 8-digit code for the Pin-Code Method. The WPS method significantly reduces the time and effort required to connect wireless devices to a network, while automatically using WPA2, the highest wireless security protocol.



In the Wi-Fi Protected Setup section, you can enable the WPS feature of this router.

You can configure the following parameters:

Enable:	Check this option to enable the Wi-Fi Protected Setup feature.
Wi-Fi Protected Setup:	This parameter displays the WPS setup status.
Reset to Unconfigured:	Click this button to disable the WPS feature used on this router.

In the **PIN Settings** section, You not only will be able to view the PIN code, but will also be able to reset the PIN to default or to generate a new PIN code. A PIN is a unique number that can be used to add the router to an existing network or to create a new network. The default PIN may be printed on the bottom of the router. For extra security, a new PIN can be generated. You can restore the default PIN at any time. Only the Administrator ("admin" account) can change or reset the PIN.

You can configure the following parameters:

PIN:	Shows the current value of the router's PIN.
Reset PIN to Default:	Click this button to restore the default PIN of the router.
Generate New PIN:	Click this button to create a random number that is a valid PIN. This becomes the router's PIN. You can then copy this PIN to You interface of the registrar.

Click the **Connect your Wireless Device** button to start Wireless Connection Setup Wizard. This wizard helps you add wireless devices to the wireless network.

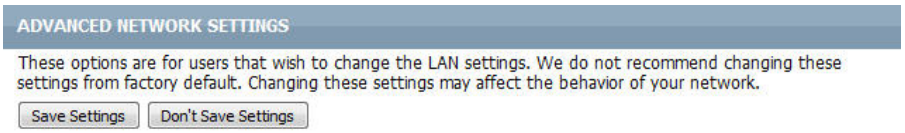
The wizard will display the wireless network settings to guide you through manual configuration, prompt you to enter the PIN for the device, or ask you to press the configuration button on the device. If the device supports Wi-Fi Protected Setup and has a configuration button, you can add it to the network by pressing the configuration button on the device and then the one on the router within 60 seconds. The status LED on the router will flash three times if the device has been successfully added to the network.

There are several ways to add a wireless device to your network. A “registrar” controls access to the wireless network and only allows devices onto the wireless network if you have entered the PIN or pressed a special Wi-Fi Protected Setup button on the device. The router acts as a registrar for the network, although other devices may act as a registrar as well.

Click the **Save Settings** button to accept the changes.
Click the **Don’t Save Settings** button to discard the changes.

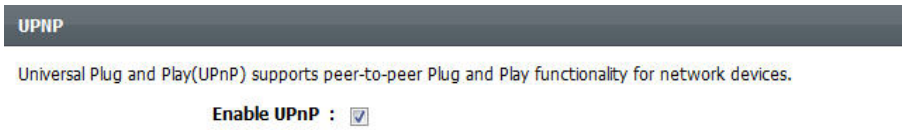
Advanced Network Settings

This section contains settings which can change the way the router handles certain types of traffic. We recommend that you not change any of these settings unless you are already familiar with them or have been instructed to change them by one of our support personnel.



UPnP:

UPnP is short for Universal Plug and Play which is a networking architecture that provides compatibility among networking equipment, software, and peripherals. The device is a UPnP enabled router, meaning it will work with other UPnP devices/ software. If you do not want to use the UPnP functionality, you can disable it by selecting "Disabled".

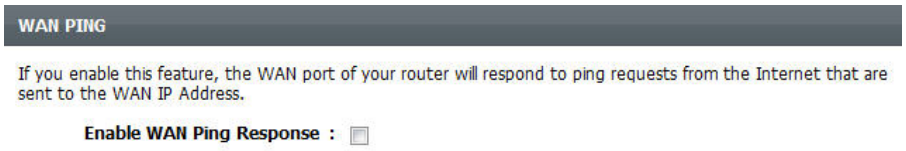


You can configure the following parameters:

Enable UPnP:	Check this option to enable the UPnP feature of the router.

WAN Ping:

When you Enable WAN Ping response, you are causing the public WAN (Wide Area Network) IP address on the device to respond to ping commands sent by Internet users. Pinging public WAN IP addresses is a common method used by hackers to test whether your WAN IP address is valid.



You can configure the following parameters:

Enable WAN Ping:	Check this option to enable the WAN Ping Response option of the router.

WAN Port Speed:

This allows you to select the speed of the WAN interface of the router. Choose from are **Auto 10/100/1000Mbps**, **10Mbps, 100Mbps, or 1000Mbps**.

You can configure the following parameters:

WAN Port Speed:	You can set the port speed of the Internet port to **Auto 10/100/1000Mbps**, **10Mbps**, **100Mbps or 1000Mbps**. Some older cable or DSL modems may require you to set the port speed to 10Mbps.

Multicast Streams:

This section enables you to allow Multicast traffic to pass from the Internet to your network more efficiently.

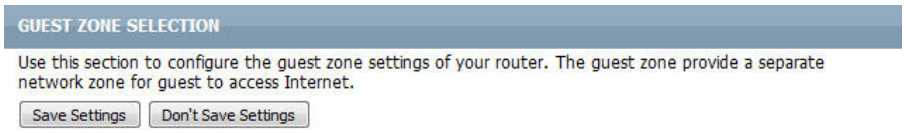
You can configure the following parameters:

Enable Multicast Streams:	Enable this option if you are receiving video on demand type of service from the Internet. The router uses the IGMP protocol to support efficient multicasting transmission of identical content, such as multimedia, from a source to a number of recipients. This option must be enabled if any applications on the LAN participate in a multicast group. If you have a multimedia LAN application that is not receiving content as expected, try enabling this option.
Wireless Enhance Mode:	Check the Wireless Enhance Mode box to enable the router to forward all multicast streams from the Internet to the wireless station using a unicast stream. This feature helps improve the quality of multimedia applications for wireless users.

Click the **Save Settings** button to accept the changes.
Click the **Don't Save Settings** button to discard the changes.

Guest Zone

On this page, you can configure the Guest Zone, settings. The guest zone provide a separate network zone for guests to access the Internet.



In the Guest Zone section below, you can to enable the routing function between guest zones.

You can configure the following parameters:

Enable Routing:	Check this option to enable routing between guest zones.

In the following section, you can configure the Guest Zone Wireless Network settings used by the **2.4GHz** frequency band.

You can configure the following parameters:

Enable Guest Zone:	Check this option to enable the Guest Zone feature for the 2.4GHz frequency band. Use the drop-down menu to schedule the time that the Firewall rule will be enabled. The schedule may be set to Always, which will allow the particular service to always be enabled. Click the New Schedule button to create your own times in the Schedules page.
Wireless Band:	Displays the frequency band used.
Wireless Network Name:	The Service Set Identifier (SSID) is the name of your wireless network. Create a name using up to 32 characters. The SSID is case-sensitive.
Security Mode:	The security mode enables You to configure wireless security for this wireless guest zone. For more information about wireless security, refer to the Wireless Settings page.

In the following section, you can configure the Guest Zone Wireless Network settings used by the **5GHz** frequency band.

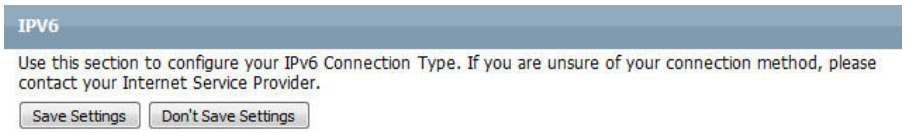
You can configure the following parameters:

Enable Guest Zone:	Check this option to enable the Guest Zone feature for the 5GHz frequency band. Use the drop-down menu to schedule the time that the Firewall rule will be enabled. The schedule may be set to Always, which will allow the particular service to always be enabled. Click the New Schedule button to create your own times in the Schedules page.
Wireless Band:	Displays the frequency band used.
Wireless Network Name:	The Service Set Identifier (SSID) is the name of your wireless network. Create a name using up to 32 characters. The SSID is case-sensitive.
Security Mode:	The security mode enables You to configure wireless security for this wireless guest zone. For more information about wireless security, refer to the Wireless Settings page.

Click the **Save Settings** button to accept the changes.
Click the **Don't Save Settings** button to discard the changes.

IPv6

On this page, you can configure the mode that the Router will use to access an IPv6 Internet connection.



There are several connection types to choose from: Link-local, Static IPv6, DHCPv6, Stateless Auto-Configuration, PPPoE, IPv6 over IPv4 Tunnel and 6to4. If you are unsure of your connection method, please contact your IPv6 ISP.

Note: If using the PPPoE option, you will need to ensure that any PPPoE client software on your computers has been removed or disabled.

IPv6 Connection Type: Static IPv6

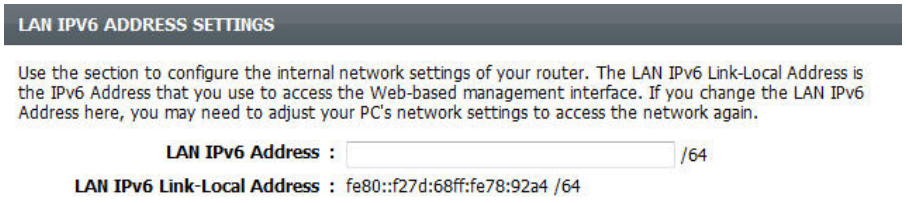
In the following section we'll discuss the parameters you can configure when setting up a Static IPv6 connection. This mode is used when your ISP provides you with a set IPv6 addresses that does not change. You must enter the IPv6 information manually into your IPv6 configuration entry fields. The information includes the IPv6 address, Subnet Prefix Length, Default Gateway, Primary DNS Server, and Secondary DNS Server. Your ISP provides you with all this information.

You can configure the following parameters:

My IPv6 Connection is:	Select the IPv6 Connection Type used for this configuration here.

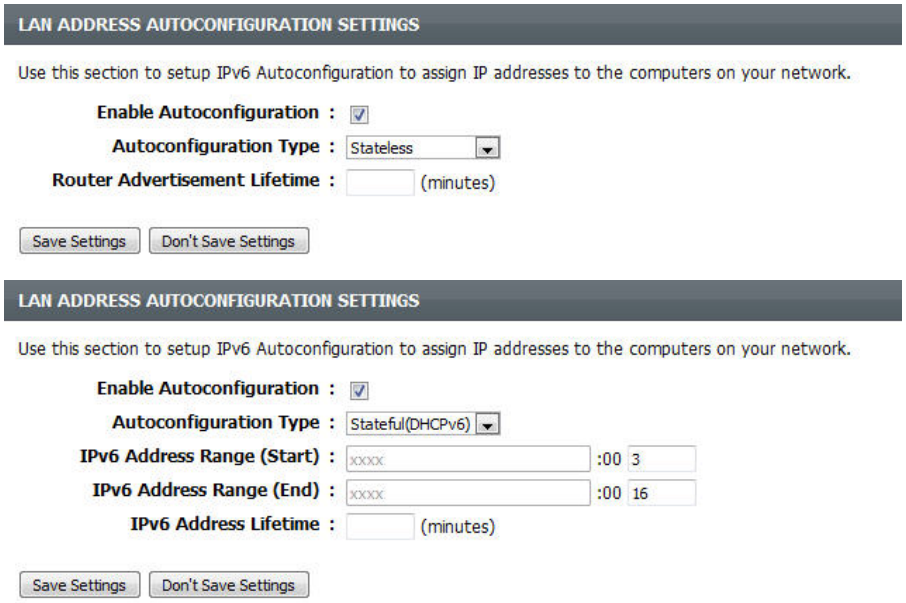
You can configure the following parameters:

IPv6 Address:	Enter the WAN IPv6 address for the router here.
Subnet Prefix Length:	Enter the WAN subnet prefix length value used here.
Default Gateway:	Enter the WAN default gateway IPv6 address used here.
Primary DNS Server:	Enter the WAN primary DNS Server address used here.
Secondary DNS Server:	Enter the WAN secondary DNS Server address used here.



You can configure the following parameters:

LAN IPv6 Address:	Enter the LAN (local) IPv6 address for the router here.
Link-Local Address:	Displays the Router's LAN Link-Local Address.



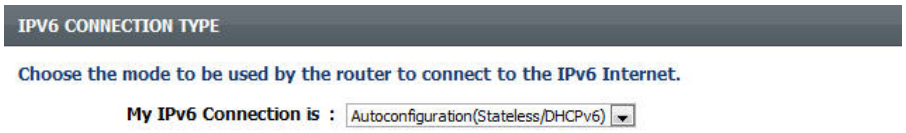
You can configure the following parameters:

Enable Auto-Configuration:	You can check this option to enable the auto-configuration feature.
Auto-Configuration Type:	You can select the auto-configuration type used here. Choose **Stateless** or **Stateful (DHCPv6)**.
Router Advertisement Lifetime:	This option is only available when the auto-configuration type is set to **Stateless**. Enter the router advertisement lifetime value here.
IPv6 Address Range (Start):	This option is only available when the auto-configuration type is set to **Stateful**. Enter the start IPv6 Address of the DHCPv6 range for your local computers.
IPv6 Address Range (End):	This option is only available when the auto-configuration type is set to **Stateful**. Enter the end IPv6 Address of the DHCPv6 range for your local computers.
IPv6 Address Lifetime:	This option is only available when the auto-configuration type is set to **Stateful**. Enter the IPv6 Address Lifetime (in minutes).

Click the **Save Settings** button to accept the changes.
Click the **Don't Save Settings** button to discard the changes.

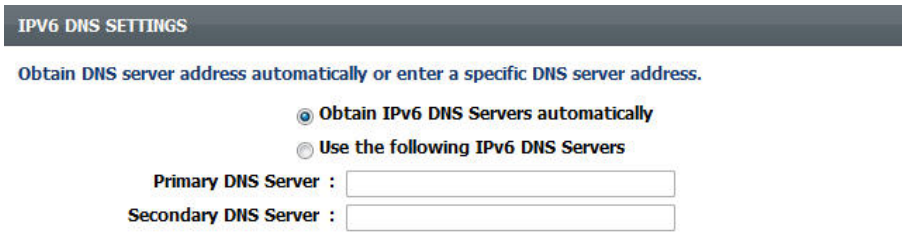
IPv6 Connection Type: Auto-Configuration (Stateless/DHCPv6)

In the following section, we'll discuss the parameters you can configure when setting up an Auto-Configuration (Stateless/DHCPv6) connection. in this connection method where the ISP assigns your IPv6 address when your router requests one from the ISP's server. Some ISP's require you to make some settings on your side before your router can connect to the IPv6 Internet.



You can configure the following parameters:

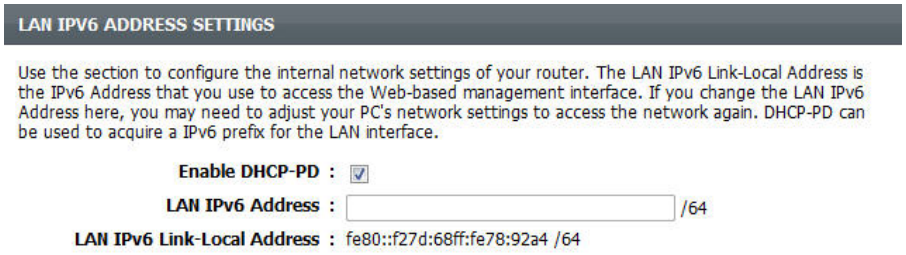
My IPv6 Connection is:	Select the IPv6 Connection Type used for this configuration here.



You can configure the following parameters:

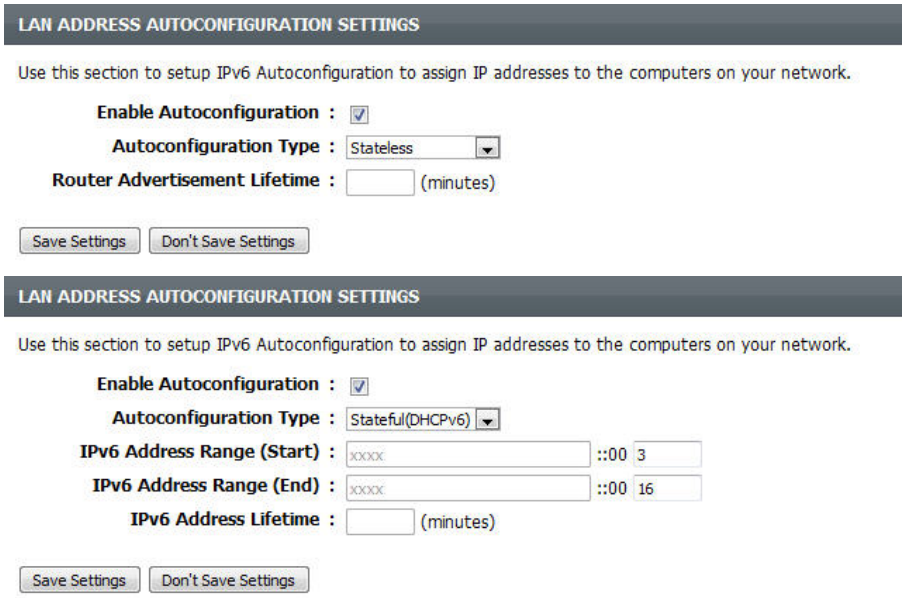
Obtain IPv6:	Select this option to obtain the DNS Server addresses automatically.
Use the following IPv6:	Select this option to manually enter the DNS Server addresses used.
Primary DNS Server:	Enter the primary DNS Server address used here.
Secondary DNS Server:	Enter the secondary DNS Server address used here.

Use this section to configure the internal network settings of your router. The LAN IPv6 Link-Local Address is the IPv6 Address that you use to access the Web-based management interface. If you change the LAN IPv6 Address here, you may need to adjust your PC's network settings to access the network again. You can use DHCP-PD to acquire a IPv6 prefix for the LAN interface.



You can configure the following parameters:

Enable DHCP PD:	Select this option to enable DHCP PD.
LAN IPv6 Address:	Enter the LAN IPv6 address used here. This address must be in the '/64' subnet.
LAN IPv6 Link-Local Address:	Displays the LAN IPv6 Link-Local address used here.



You can configure the following parameters:

Enable Auto-Configuration:	You can check this option to enable the auto-configuration feature.
Auto-Configuration Type:	You can select the auto-configuration type used here. Choose **Stateless** or **Stateful (DHCPv6)**.
Router Advertisement Lifetime:	This option is only available when the auto-configuration type is set to **Stateless**. Enter the router advertisement lifetime value used here.
IPv6 Address Range (Start):	This option is only available when the auto-configuration type is set to **Stateful**. Enter the start IPv6 Address of the DHCPv6 range for your local computers.
IPv6 Address Range (End):	This option is only available when the auto-configuration type is set to **Stateful**. Enter the end IPv6 Address of the DHCPv6 range for your local computers.
IPv6 Address Lifetime:	This option is only available when the auto-configuration type is set to **Stateful**. Enter the IPv6 Address Lifetime (in minutes).

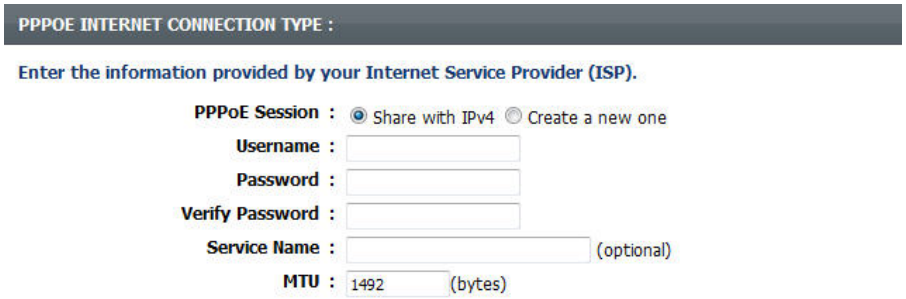
Click the **Save Settings** button to accept the changes.
Click the **Don't Save Settings** button to discard the changes.

IPv6 Connection Type: PPPoE

Select this option if your ISP requires you to use a PPPoE (Point to Point Protocol over Ethernet) connection to IPv6 Internet. DSL providers typically use this option. This method of connection requires you to enter a Username and Password (provided by your Internet Service Provider) to gain access to the IPv6 Internet. The supported authentication protocols are PAP and CHAP.

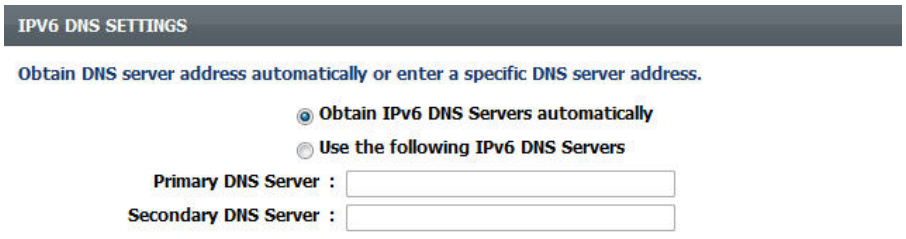
You can configure the following parameters:

My IPv6 Connection is:	Select the IPv6 Connection Type used for this configuration here.



You can configure the following parameters:

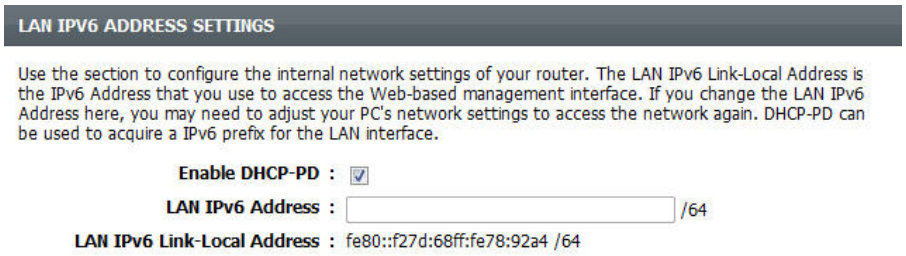
PPPoE Session:	Select the PPPoE Session value used here. This option will state that this connection shares it's information with the already configured IPv6 PPPoE connection, or You can create a new PPPoE connection here.
Username:	Enter the PPPoE username used here. This information is obtainable from the ISP.
Password:	Enter the PPPoE password used here. This information is obtainable from the ISP.
Verify Password:	Re-enter the PPPoE password used here.
Service Name:	Enter the service name for this connection here. This option is optional.
MTU:	Enter the MTU value used here. The default value is 1492.



You can configure the following parameters:

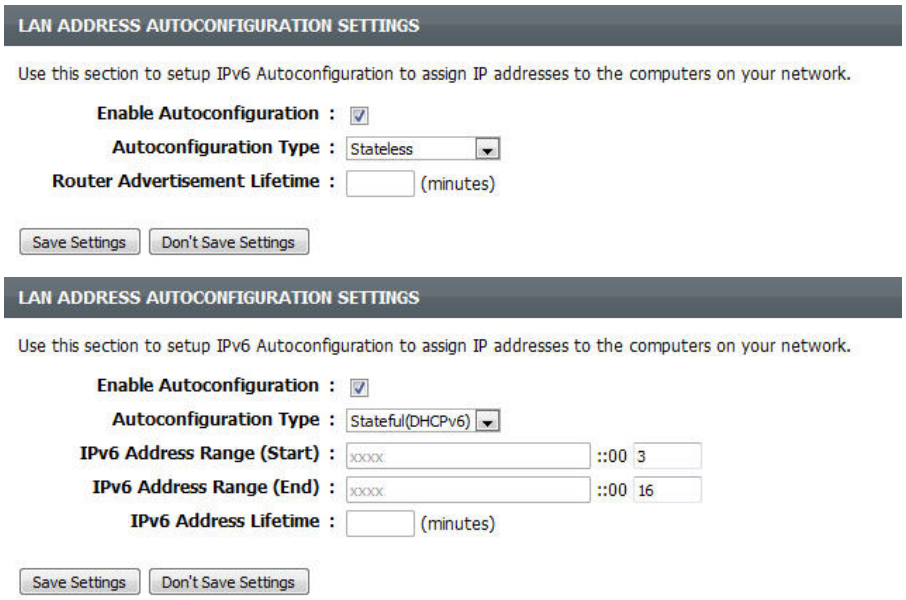
Obtain IPv6:	Select this option to obtain the DNS Server addresses automatically.
Use the following IPv6:	Select this option to manually enter the DNS Server addresses used.
Primary DNS Server:	Enter the primary DNS Server address used here.
Secondary DNS Server:	Enter the secondary DNS Server address used here.

Use this section to configure the internal network settings of your router. The LAN IPv6 Link-Local Address is the IPv6 Address that you use to access the Web-based management interface. If you change the LAN IPv6 Address here, you may need to adjust your PC's network settings to access the network again. You can use DHCP-PD to acquire a IPv6 prefix for the LAN interface.



You can configure the following parameters:

Enable DHCP PD:	Select this option to enable DHCP PD.
LAN IPv6 Address:	Enter the LAN IPv6 address used here. This address must be in the '/64' subnet.
LAN IPv6 Link-Local Address:	Displays the LAN IPv6 Link-Local address used here.



You can configure the following parameters:

Auto-Configuration:	You can check this option to enable the auto-configuration feature.
Auto-Configuration Type:	You can select the auto-configuration type used here. Choose **Stateless** or **Stateful (DHCPv6)**.
Router Advertisement Lifetime:	This option is only available when the auto-configuration type is set to **Stateless**. Enter the router advertisement lifetime value used here.
IPv6 Address Range (Start):	This option is only available when the auto-configuration type is set to **Stateful**. Enter the start IPv6 Address of the DHCPv6 range for your local computers.
IPv6 Address Range (End):	This option is only available when the auto-configuration type is set to **Stateful**. Enter the end IPv6 Address of the DHCPv6 range for your local computers.
IPv6 Address Lifetime:	This option is only available when the auto-configuration type is set to **Stateful**. Enter the IPv6 Address Lifetime (in minutes).

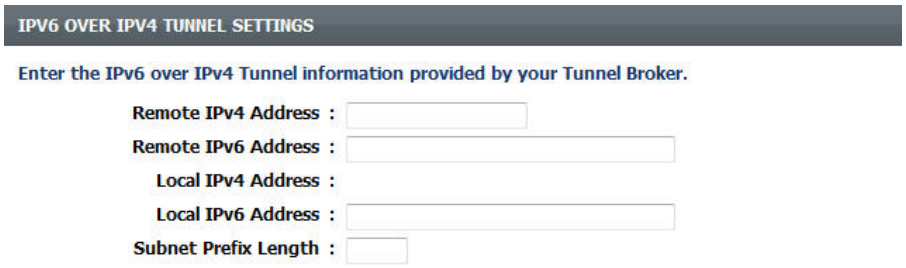
Click the **Save Settings** button to accept the changes.
Click the **Don't Save Settings** button to discard the changes.

IPv6 Connection Type: IPv6 in IPv4 Tunnel

In this section, you can configure the IPv6 connection to run in IPv4 Tunnel mode. IPv6 over IPv4 tunneling encapsulates IPv6 packets in IPv4 packets so that IPv6 packets can be sent over an IPv4 infrastructure.

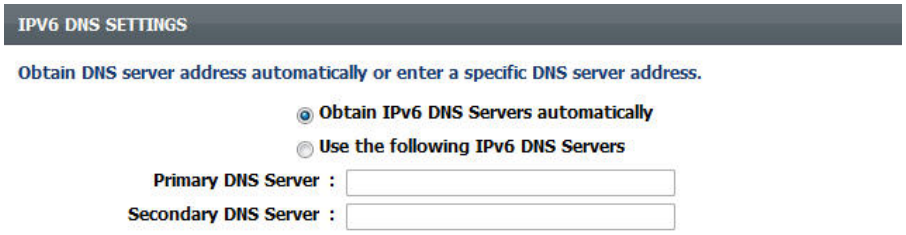
You can configure the following parameters:

My IPv6 Connection is:	Select the IPv6 Connection Type used for this configuration here.



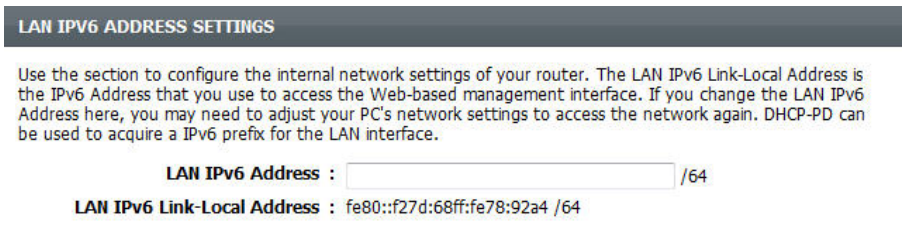
You can configure the following parameters:

Remote IPv4 Address:	Enter the remote IPv4 address used here.
Remote IPv6 Address:	Enter the remote IPv6 address used here.
Local IPv4 Address:	Enter the local IPv4 address used here.
Local IPv6 Address:	Enter the local IPv6 address used here.
Subnet Prefix Length:	Enter the Subnet prefix length value used here.



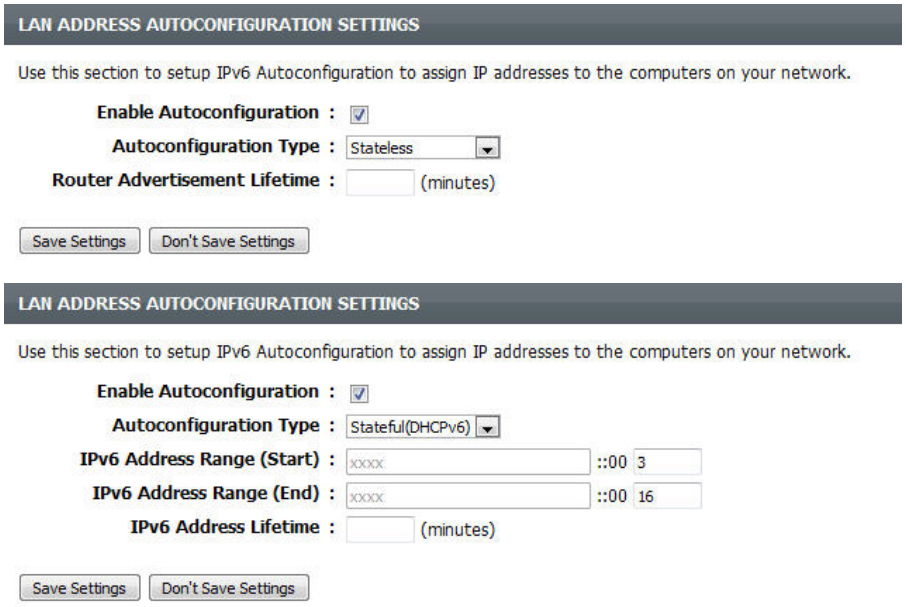
You can configure the following parameters:

Obtain IPv6:	Select this option to obtain the DNS Server addresses automatically.
Use the following IPv6:	Select this option to manually enter the DNS Server addresses used.
Primary DNS Server:	Enter the primary DNS Server address used here.
Secondary DNS Server:	Enter the secondary DNS Server address used here.



You can configure the following parameters:

LAN IPv6 Address:	Enter the LAN IPv6 address used here. This address must be in the '/64' subnet.
LAN IPv6 Link-Local:	Displays the LAN IPv6 Link-Local address used here.



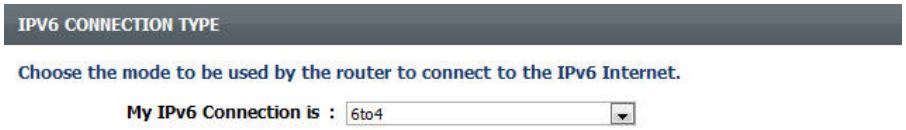
You can configure the following parameters:

Auto-Configuration:	You can check this option to enable the auto-configuration feature.
Auto-Configuration Type:	You can select the auto-configuration type used here. Choose **Stateless** or **Stateful (DHCPv6)**.
Router Advertisement Lifetime:	This option is only available when the auto-configuration type is set to **Stateless**. Enter the router advertisement lifetime value used here.
IPv6 Address Range (Start):	This option is only available when the auto-configuration type is set to **Stateful**. Enter the start IPv6 Address of the DHCPv6 range for your local computers.
IPv6 Address Range (End):	This option is only available when the auto-configuration type is set to **Stateful**. Enter the end IPv6 Address of the DHCPv6 range for your local computers.
IPv6 Address Lifetime:	This option is only available when the auto-configuration type is set to **Stateful**. Enter the IPv6 Address Lifetime (in minutes).

Click the **Save Settings** button to accept the changes.
Click the **Don't Save Settings** button to discard the changes.

IPv6 Connection Type: 6to4

In this section, you can configure the IPv6 6to4 connection settings. 6to4 is an IPv6 address assignment and automatic tunneling technology that is used to provide unicast IPv6 connectivity between IPv6 sites and hosts across the IPv4 Internet.

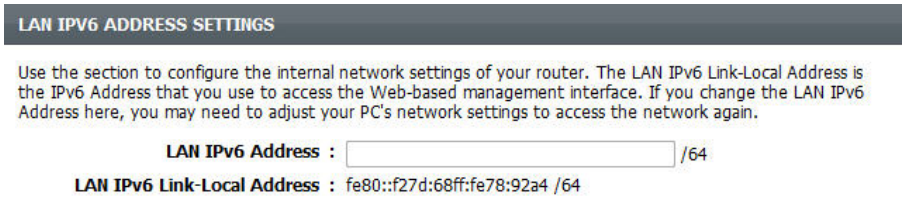


You can configure the following parameters:

My IPv6 Connection is:	Select the IPv6 Connection Type used for this configuration here.

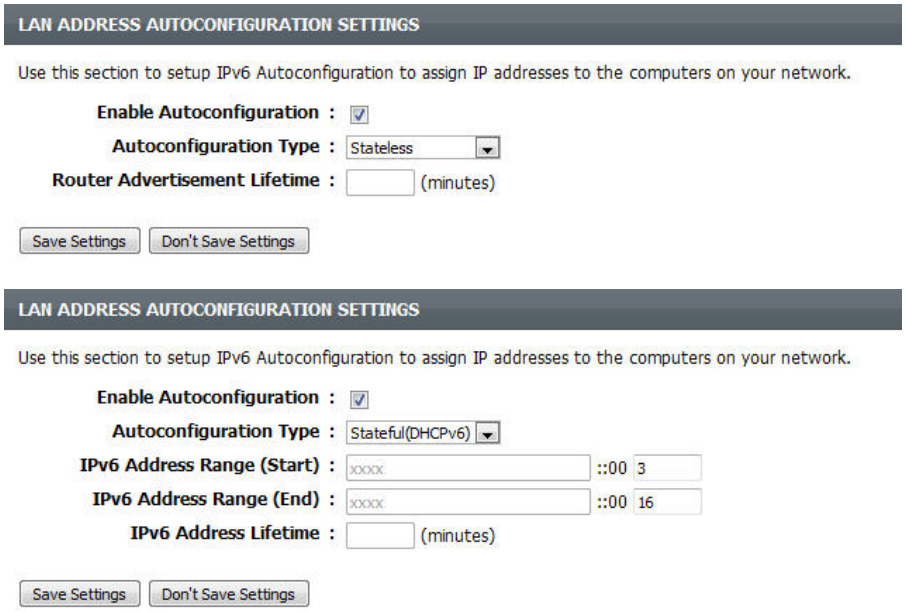
You can configure the following parameters:

6to4 Address:	Displays the 6to4 configured address.
6to4 Relay:	Enter the 6to4 relay address used here.
Primary DNS Server:	Enter the primary DNS Server address used here.
Secondary DNS Server:	Enter the secondary DNS Server address used here.



You can configure the following parameters:

LAN IPv6 Address:	Enter the LAN IPv6 address used here. This address must be in the '/64' subnet.
LAN IPv6 Link-Local Address:	Displays the LAN IPv6 Link-Local address used here.



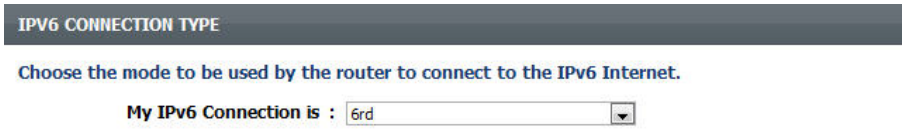
You can configure the following parameters:

Auto-Configuration:	You can check this option to enable the auto-configuration feature.
Auto-Configuration Type:	You can select the auto-configuration type used here. Choose **Stateless** or **Stateful (DHCPv6)**.
Router Advertisement Lifetime:	This option is only available when the auto-configuration type is set to **Stateless**. Enter the router advertisement lifetime value used here.
IPv6 Address Range (Start):	This option is only available when the auto-configuration type is set to **Stateful**. Enter the start IPv6 Address of the DHCPv6 range for your local computers.
IPv6 Address Range (End):	This option is only available when the auto-configuration type is set to **Stateful**. Enter the end IPv6 Address of the DHCPv6 range for your local computers.
IPv6 Address Lifetime:	This option is only available when the auto-configuration type is set to **Stateful**. Enter the IPv6 Address Lifetime (in minutes).

Click the **Save Settings** button to accept the changes.
Click the **Don't Save Settings** button to discard the changes.

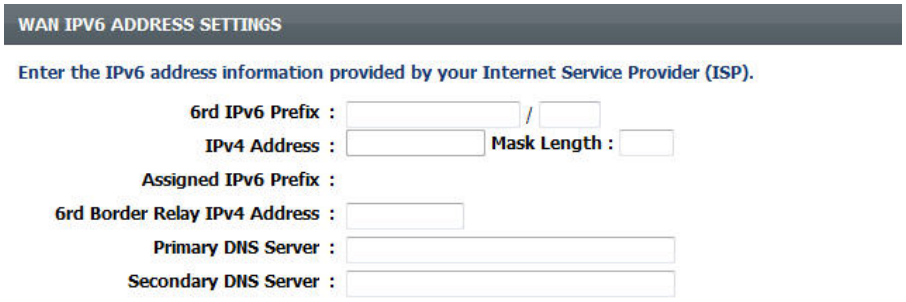
IPv6 Connection Type: 6rd

In this section, you can configure the IPv6 6rd connection settings.



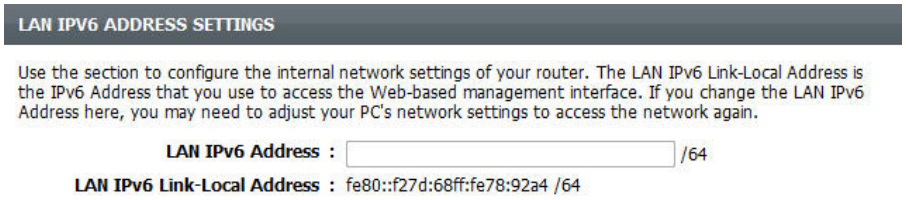
You can configure the following parameters:

My IPv6 Connection is:	Select the IPv6 Connection Type used for this configuration here.



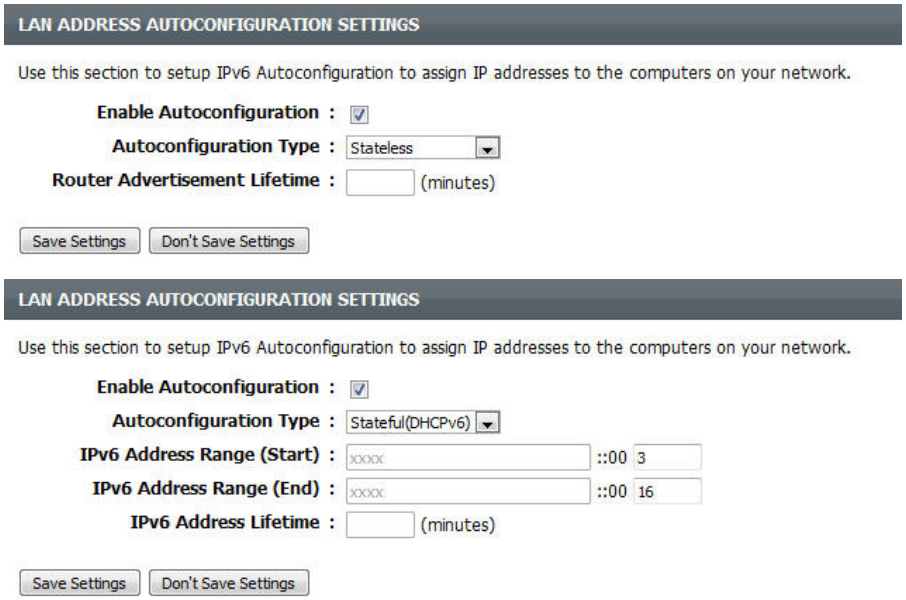
You can configure the following parameters:

6rd IPv6 Prefix:	Enter the 6rd IPv6 address and prefix value used here.
IPv4 Address:	Enter the IPv4 address used here.
Mask Length:	Enter the IPv4 mask length used here.
Assigned IPv6 Prefix:	Displays the IPv6 assigned prefix value.
6rd Border Relay IPv4 Address:	Enter the 6rd border relay IPv4 address used here.
Primary DNS Server:	Enter the primary DNS Server address used here.
Secondary DNS Server:	Enter the secondary DNS Server address uses here.



You can configure the following parameters:

LAN IPv6 Address:	Enter the LAN IPv6 address used here. This address must be in the '/64' subnet.
LAN IPv6 Link-Local Address:	Displays the LAN IPv6 Link-Local address used here.



You can configure the following parameters:

Auto-Configuration:	You can check this option to enable the auto-configuration feature.
Auto-Configuration Type:	You can select the auto-configuration type used here. Choose **Stateless** or **Stateful (DHCPv6)**.
Router Advertisement Lifetime:	This option is only available when the auto-configuration type is set to **Stateless**. Enter the router advertisement lifetime value used here.
IPv6 Address Range (Start):	This option is only available when the auto-configuration type is set to **Stateful**. Enter the start IPv6 Address of the DHCPv6 range for your local computers.
IPv6 Address Range (End):	This option is only available when the auto-configuration type is set to **Stateful**. Enter the end IPv6 Address of the DHCPv6 range for your local computers.
IPv6 Address Lifetime:	This option is only available when the auto-configuration type is set to **Stateful**. Enter the IPv6 Address Lifetime (in minutes).

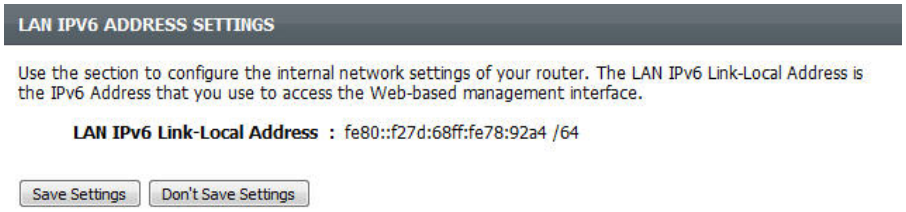
Click the **Save Settings** button to accept the changes.
Click the **Don't Save Settings** button to discard the changes.

IPv6 Connection Type: Link-Local Only

The Link-local address is used by nodes and routers when communicating with neighboring nodes on the same link. This mode enables IPv6-capable devices to communicate with each other on the LAN side.

You can configure the following parameters:

My IPv6 Connection is:	Select the IPv6 Connection Type used for this configuration here.



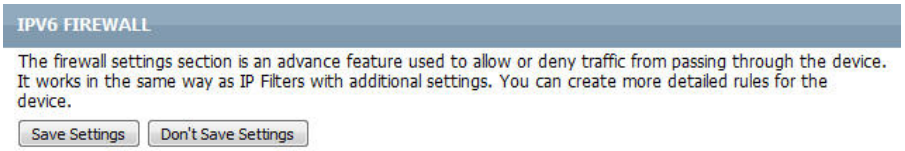
You can configure the following parameters:

LAN IPv6 Link-Local Address:	Displays the LAN IPv6 Link-Local address used.

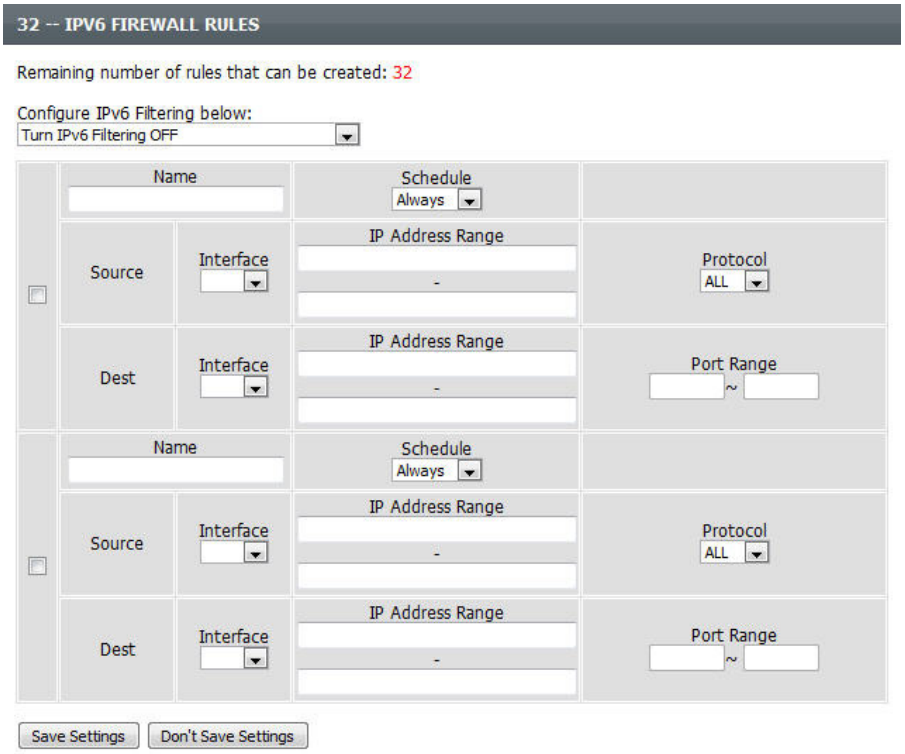
Click the **Save Settings** button to accept the changes.
Click the **Don't Save Settings** button to discard the changes.

IPv6 Firewall

On this page, you can configure the IPv6 firewall settings. The firewall settings section is an advance feature that is used to allow or deny traffic from passing through the device. It works in the same way as IP Filters, but with additional settings. You can create more detailed rules for the device.



In the IPv6 Firewall rules section you can create, enable and disable IPv6 firewall rules used by this device.

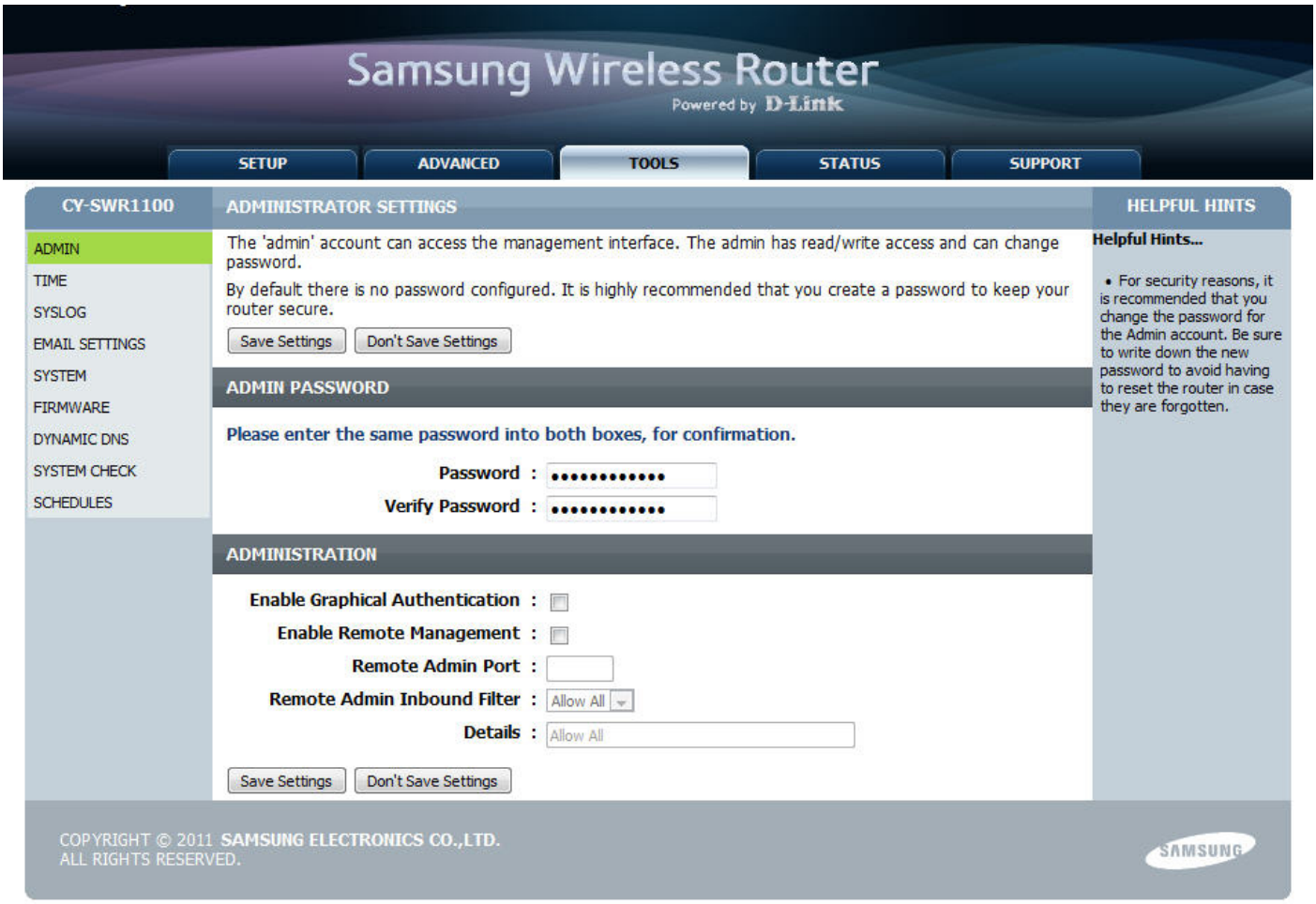


You can configure the following parameters:

Configure IPv6 Filtering:	This option defines the behaviour of all the IPv6 firewall rules created. Choose '**Turn IPv6 Filtering OFF**', '**Turn IPv6 Filtering ON and ALLOW rules listed**', or '**Turn IPv6 Filtering ON and DENY rules listed**'. Select the appropriate option used here.
Checkbox:	Check this option to use the firewall rules created.
Name:	Enter a custom firewall rule name here. This name is used for identification.
Source Interface:	Select the source interface used here.
Destination Interface:	Select the destination interface used here.
Schedule:	Select a time schedule that will be applied to this rules here.
IP Address Range:	Enter the IPv6 address range used here.
Protocol:	Select the protocol used for this rule here. Choose **ALL**, **TCP**, **UDP**, or **ICMP**.
Port Range:	Enter the port range used for this rule here.

Click the **Save Settings** button to accept the changes.
Click the **Don't Save Settings** button to discard the changes.

Tools Tab



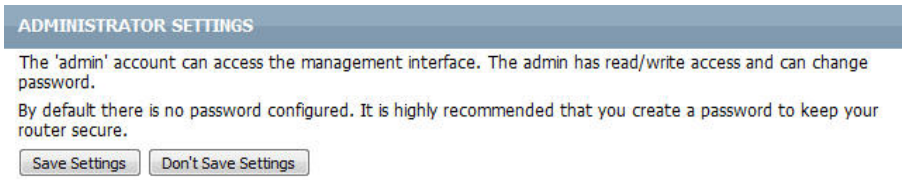
On this Tab, you will be able to configure features that are related to the router itself such as the time settings, login accounts, firmware update and more.

You can configure the following pages on the Tools Tab:

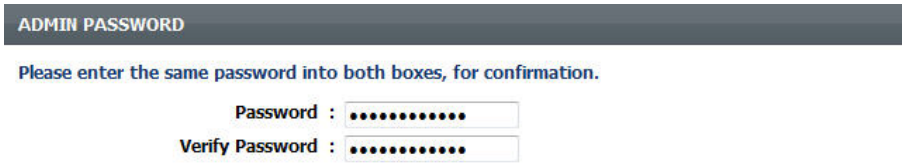
- **Administration:** On this page, you can configure a new password as well as remote administration settings for this device.
- **Time:** On this page, you can configure the time and date settings for this router.
- **System Log:** On this page, you can view and configure the system log.
- **EMail Settings:** On this page, you can configure the email settings for this router.
- **System:** On this page, you can reboot, reset, backup and restore this router.
- **Firmware:** On this page, you can perform a firmware upgrade on this router.
- **Dynamic DNS:** On this page, you can configure the DDNS settings for this router.
- **System Check:** On this page, you can perform and system check (using Ping) for this router.
- **Schedules:** On this page, you can create and maintain time schedules for this router.

ADMIN

This page allows you to change the Administrator password and configure the authentication settings. This page also allows you to enable Remote Management via the Internet.

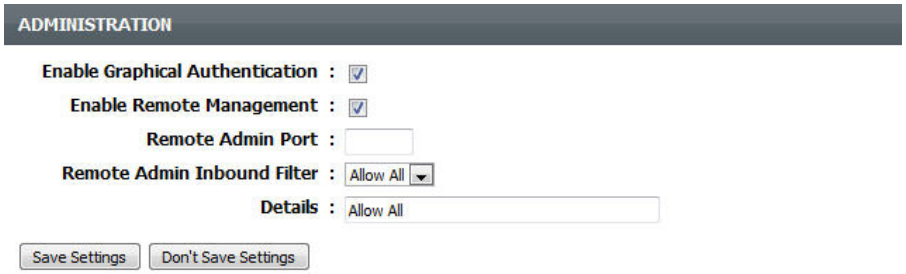


In the **Admin Password** section, you can change the login password for this device.



You can configure the following parameters:

Password:	Enter the new login password here.
Verify Password:	Re-enter the new login password here.



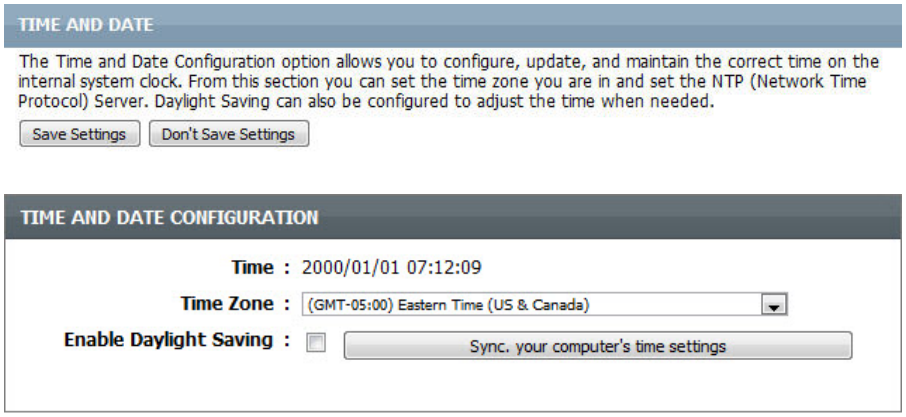
You can configure the following parameters:

Enable Graphical Authentication:	Check this option to enable the graphical image confirmation when you login to the web configuration. Example: 
Enable Remote Management:	Check this option to enable remote management. This option will enable the router to be accessible from the Internet port.
Remote Admin Port:	Enter the remote administration port number used here. Sometimes services such as an internal webserver will occupy the port number 80. In this option, you can change the remote administration port to 8080 for example.
Remote Admin Inbound Filter:	Select the appropriate remote admin inbound filter behavior here. Choose **Allow All** and **Deny All**.
Details:	Enter the remote admin inbound filter detail description here.

Click the **Save Settings** button to accept the changes.
Click the **Don't Save Settings** button to discard the changes.

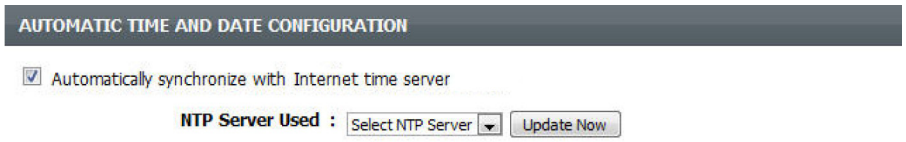
TIME

The Time page allows you to configure, update, and maintain the correct time on the internal system clock. On this page, you can set your time zone and the Time Server. You can configure Daylight Saving to adjust the time automatically when needed.



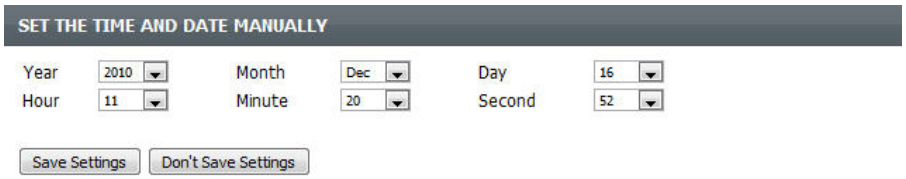
You can configure the following parameters:

Time:	Displays the current time configuration running on this device.
Time Zone:	Select the your time zone.
Enable Daylight Saving:	Check this box if the country your are located in uses Daylight Savings time. Enter a daylight savings time. start date and an end date.
Sync. your computer's time settings:	Click this button to synchronize the router's system clock to the management computer's time settings.



You can configure the following parameters:

Automatically synchronize:	NTP is short for Network Time Protocol. NTP synchronizes computer clock times in a network of computers. Check this option to enable automatic time and date synchronizing.
NTP Server Used:	Select the NTP server. The interval at which the router will communicate with the NTP server is set to 7 days.
Update Now:	Click this button to update the current time and date of the router.



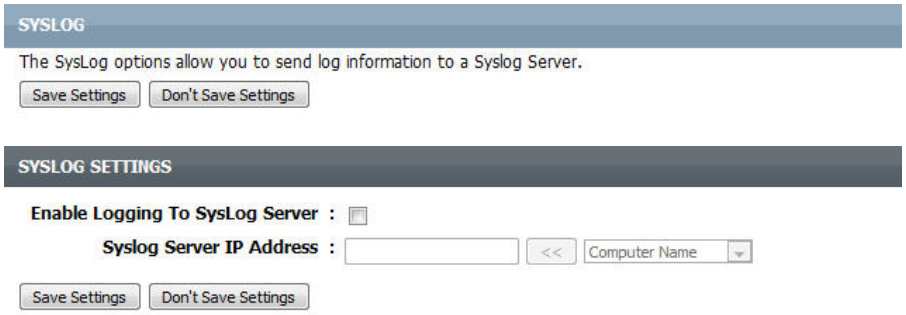
You can configure the following parameters:

Set Manually:	Here you can manually configure the date and time used by this device. Options to configure are **Year**, **Month**, **Day**, **Hour**, **Minute**, and **Second**.

Click the **Save Settings** button to accept the changes.
Click the **Don't Save Settings** button to discard the changes.

SYSLOG

The Syslog options allow you to send log information to a System Log Server.



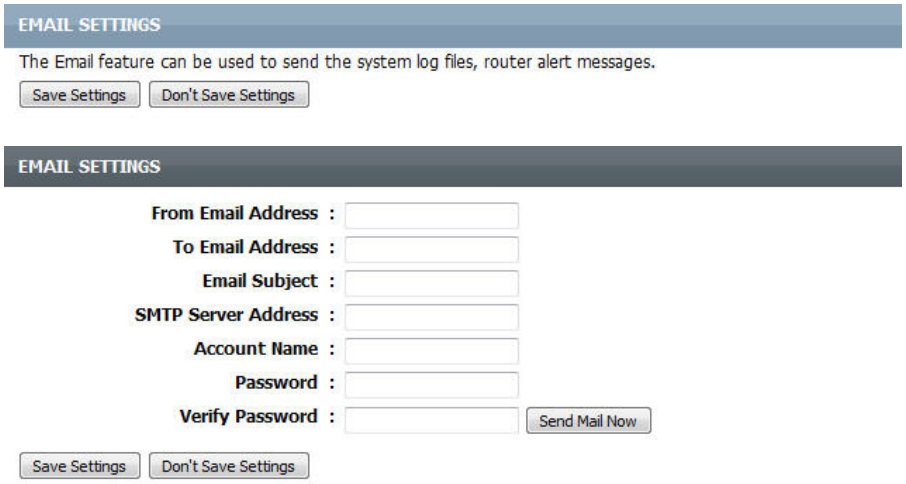
You can configure the following parameters:

Enable Logging:	Check this option to enable the Syslog feature.
Syslog Server IP Address:	Enter the Syslog Server IP address here.

Click the **Save Settings** button to accept the changes.
Click the **Don't Save Settings** button to discard the changes.

Email Settings

You can use the Email feature to send the system log files and router alert messages to your email address.



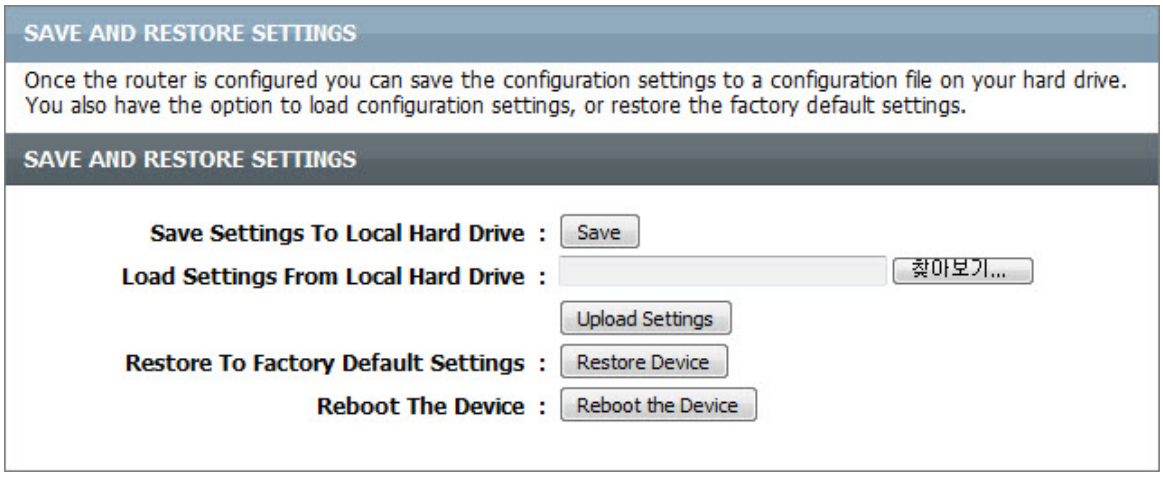
You can configure the following parameters:

From Email Address:	This email address will appear as the sender when you receive a log file or firmware upgrade notification via email.
To Email Address:	Enter the email address to which you want the email sent.
Email Subject:	Enter the text that you want to appear in the subject line of the e-mail sent.
SMTP Server Address:	Enter the SMTP e-mail server address. If your SMTP server requires authentication, select this option.
Account Name:	Enter your email account name.
Password:	Enter the password associated with the account.
Verify Password:	Re-enter the password associated with the account.
Send Mail Now:	Click this button to send a test email from the Router to verify that the email settings have been configured correctly.

Click the **Save Settings** button to accept the changes.
Click the **Don't Save Settings** button to discard the changes.

System

This section allows you to manage the router's configuration settings, reboot the router, and restore the router to the factory default settings. Restoring the unit to the factory default settings will erase all settings, including any rules that you've created.



You can configure the following parameters:

Save Settings To Local Hard Drive:	Use this option to save the current router configuration settings to a file on the hard disk of the computer you are using. First, click the Save button. A file dialog will appear allowing you to select a file name for the settings and a location to saver them to.
Load Settings From Local Hard Drive:	Use this option to load previously saved router configuration settings. First, use the **Browse** option to find a previously saved file of configuration settings. Then, click the **Upload Settings** button below to transfer those settings to the router.
Restore To Factory Default Settings:	This option will restore all configuration settings to the settings that were in effect at the time the router was shipped from the factory. Any settings that have not been saved will be lost, including any rules that you have created. If you want to save the current router configuration settings, use the Save button above.
Reboot The Device:	Click to reboot the router.

Click the **Save Settings** button to accept the changes.
Click the **Don't Save Settings** button to discard the changes.

FIRMWARE

Use the Firmware window to upgrade the firmware of the Router and install language packs. If you plan to install new firmware, make sure the firmware you want to use is on the local hard drive of the computer. If you want to install a new language pack, make sure that you have the language pack available. Please check the support site for firmware updates. You can download firmware upgrades to your hard drive from the support site.

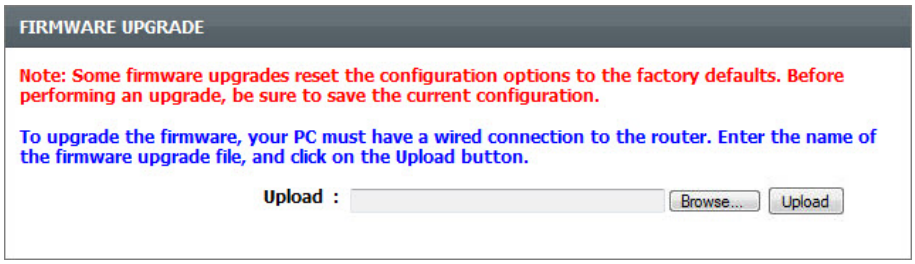
※You can also download firmware upgrades from www.samsung.com

In the **Firmware Information** section, you can view the **Current Firmware Version** number running on this device and the **Current Firmware Date** of this firmware.

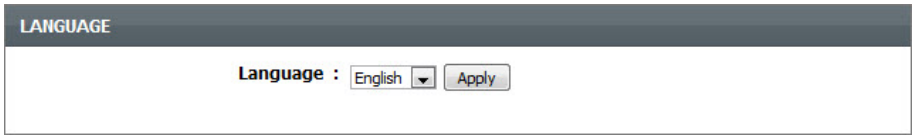
In the Firmware Upgrade section, you can physically upgrade the firmware of this device by clicking on the Browse button, navigating to the firmware file, and saving the file on your local hard drive. After locating the file on your local disk, click the Upload button to initiate the firmware upgrade.

⚠	**Note:** Some firmware upgrades will reset the configuration of the device to factory defaults. Be sure to save the current configuration first before running a firmware update.

⚠	**Note:** Always update the firmware of this device using a **wired** connection. Never upgrade the firmware using a wireless connection.



In the **Language** section, you can change the router's language.

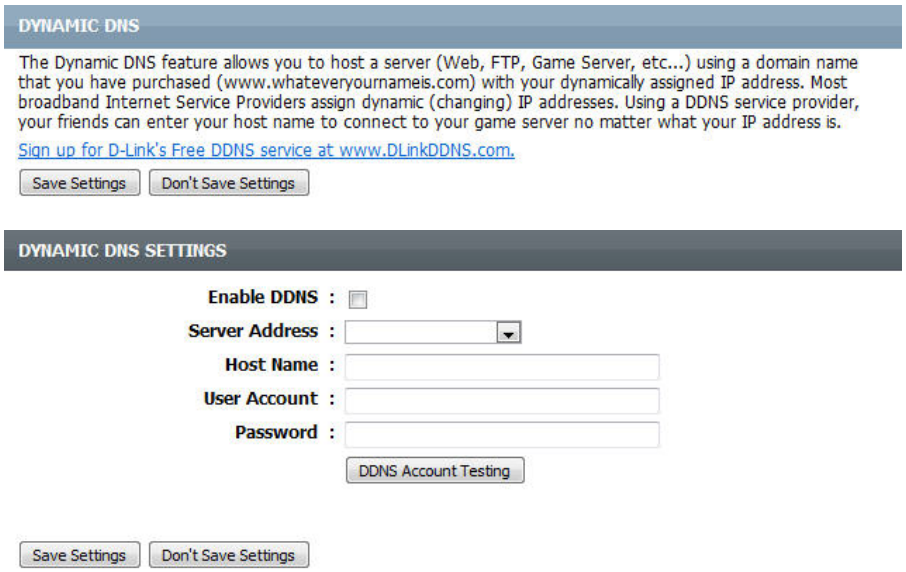


Always keep a close lookout on the local vendor's website for new firmware upgrades and language packs.

Click the **Save Settings** button to accept the changes.
Click the **Don't Save Settings** button to discard the changes.

Dynamic DNS

The DDNS feature allows you to host a server (Web, FTP, Game Server, etc…) using a domain name that you have purchased (www.whateveryournameis.com) with your dynamically assigned IP address. Most broadband Internet Service Providers assign dynamic (changing) IP addresses. Using a DDNS service provider, your friends can enter in your domain name to connect to your server no matter what your IP address is.



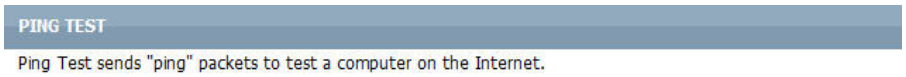
You can configure the following parameters:

Enable DDNS:	Dynamic Domain Name System is a method of keeping a domain name linked to a changing IP Address. Check the box to enable DDNS.
Server Address:	Choose your DDNS provider from the drop down menu.
Host Name:	Enter the Host Name that you registered with your DDNS service provider.
User Account:	Enter Youname for your DDNS account.
Password:	Enter the Password for your DDNS account.
DDNS Account Testing:	Click this button to verify that the DDNS account user name and password have been entered correctly.

Click the **Save Settings** button to accept the changes.
Click the **Don't Save Settings** button to discard the changes.

System Check

You can use this useful diagnostic utility to check if a computer is on the Internet. It sends ping packets.



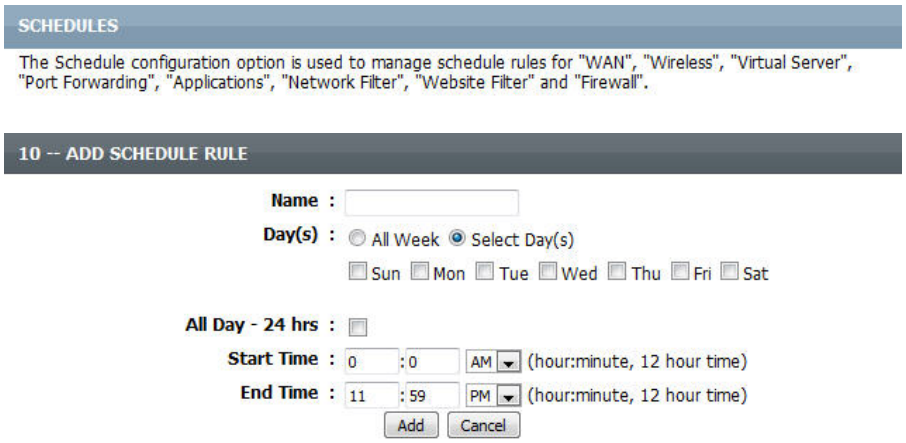
In the **Ping Test** section, you can test the Internet connectivity by entering in a **host name** or the **IP address** that you want to ping (Packet Internet Groper), and then Click the **Ping** button. The status of your Ping attempt will be displayed in the **Ping Result** box.

In the **IPv6 Ping Test** section, you can test the Internet connectivity by entering a **host name** or the **IPv6 address** that you want to ping (Packet Internet Groper), and then Click the **Ping** button. The status of your Ping attempt will be displayed in the **Ping Result** box.

The results of the attempted ping is displayed in the Ping Result section.

SCHEDULES

You can create schedules for use with rules. For example, if you want to restrict web access to Mon-Fri from 3pm to 8pm, you could create a schedule selecting Mon, Tue, Wed, Thu, and Fri and enter a Start Time of 3pm and End Time of 8pm.

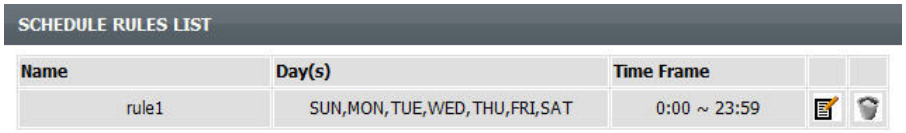


You can configure the following parameters:

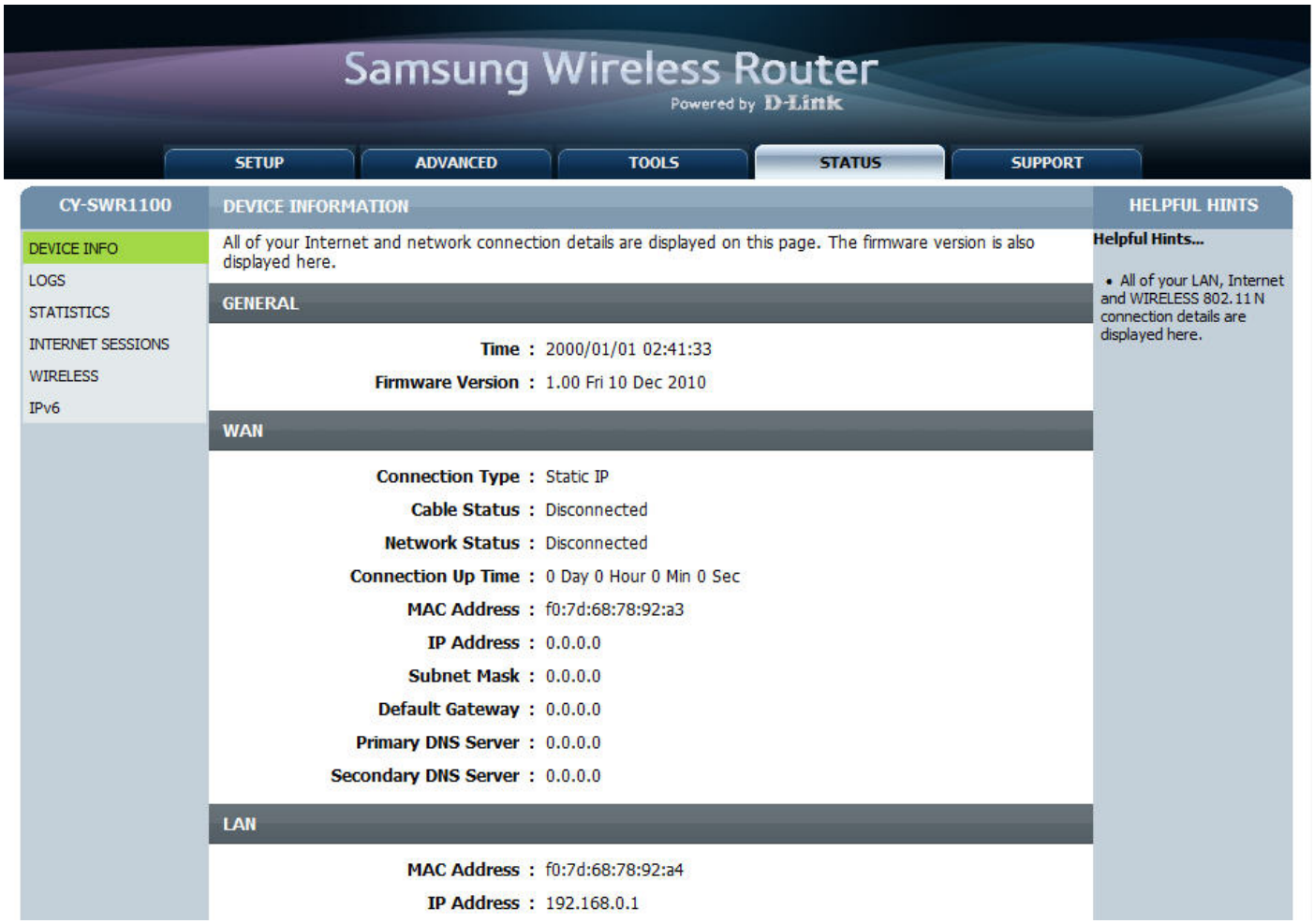
Name:	Enter the custom name for the new schedule rule here. This name is used for identification.
Day(s):	To use every day in the week for this rule, select the **All Week** option. To use only selected days for this rule, select the **Select Day(s)** option, and then check the days you want to apply the rule.
All Day - 24 hrs:	To enable a rule to run 24 hours instead of only a certain part of the day, check this option.
Start Time:	If you don't select the **All Day** option, you can enter the starting time here.
End Time:	If you don't select the **All Day** option, you can enter the ending time here.

Click the **Add** button to add this new rule to the schedule rules list.
Click the **Cancel** button to discard the information and cancel the rule addition.

In the **Schedule Rules List** section, you can view the available schedule rules created. To edit an existing rule, click the icon of the specific entry. To remove an existing rule, click the icon of the specific entry.



Status Tab



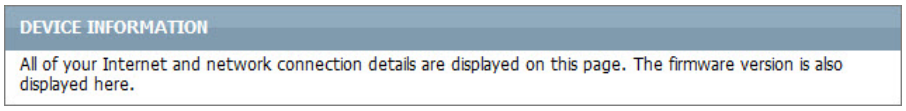
On this Tab, you can view information regarding the configuration and functionality of this device. Displays like WAN, LAN and Wireless configurations, System, Firewall and Router logs, and more.

You can configure the following pages on the Status Tab:

- **Device Information:** This page displays the current information for the router. It will display the LAN, WAN (Internet), and Wireless information.
- **Logs:** The Logs option allows you to view the router logs. You can define what types of events you want to view and the level of the events to view. This router also has external Syslog Server support so you can send the log files to a computer on your network that is running a Syslog utility.
- **Statistics:** You can view the number of packets that pass through the router on both the WAN and LAN ports and both the 802.11n/g (2.4GHz) and 802.11n/a (5GHz) wireless bands. The traffic counter will reset if the device is rebooted.
- **Internet Sessions:** The Internet Sessions page displays full details of active Internet sessions through your router. An Internet session is a conversation between a program or application on a LAN-side computer and a program or application on a WAN-side computer.
- **Wireless:** The wireless client table displays a list of current connected wireless clients. This table also displays the connection time and MAC address of the connected wireless clients.
- **IPv6:** The IPv6 page displays a summary of the Router's IPv6 settings and lists the IPv6 address and host name of any IPv6 clients.

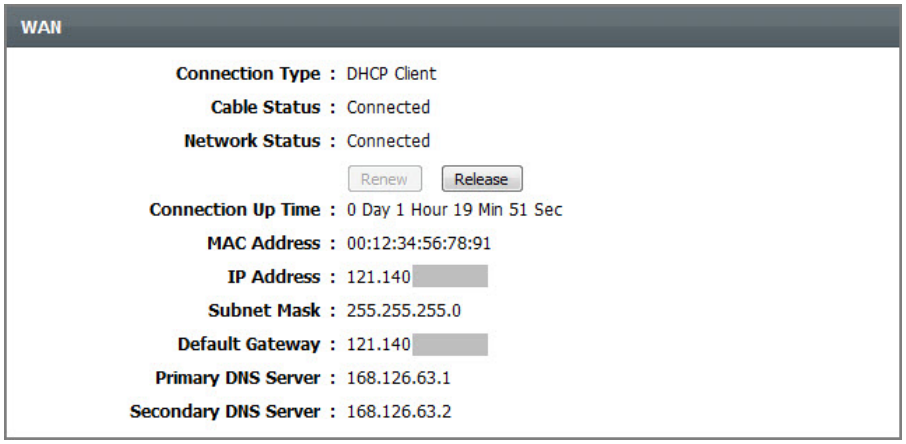
Device Info

This page displays the current information for the router. It will display the LAN, WAN (Internet), and Wireless information. If your Internet connection is set up for a Dynamic IP address, then a Release button and a Renew button will be displayed. Use Release to disconnect from your ISP and use Renew to connect to your ISP.

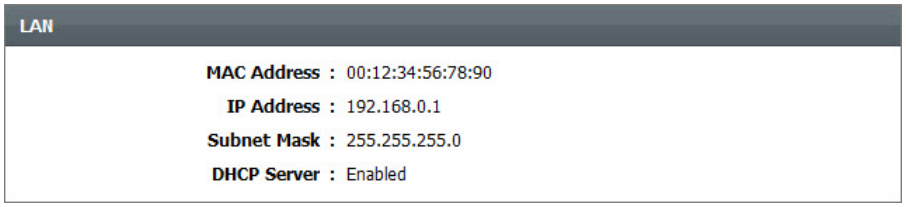


In the **General** section, information about the time and firmware is being displayed.

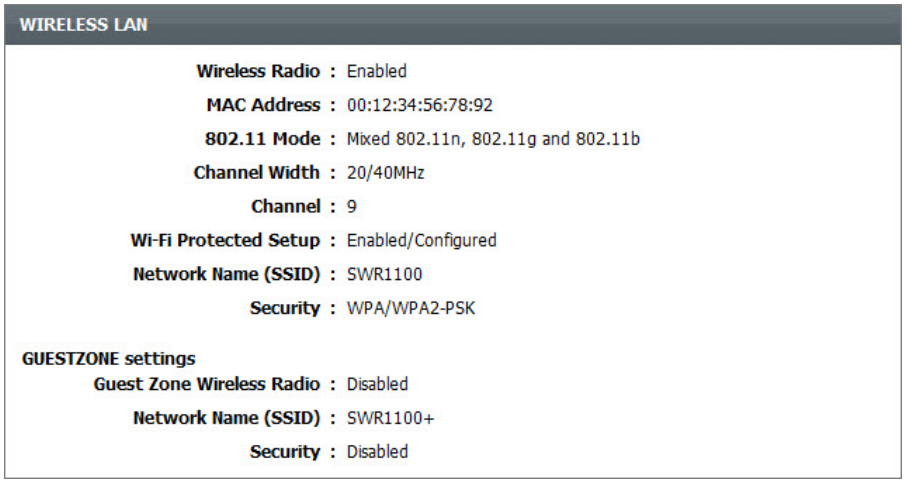
In the **WAN** section, information about the Internet connection is displayed.



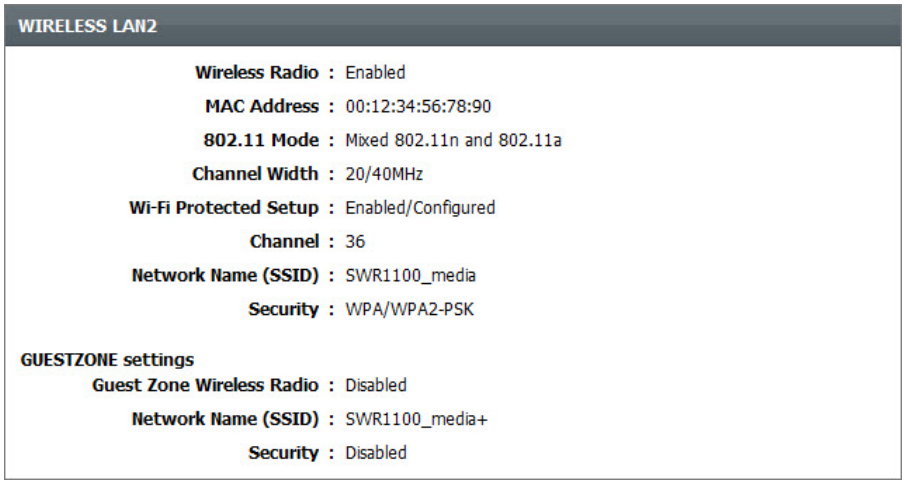
In the **LAN** section, information about the Local Area Network configuration is displayed.



In the **Wireless LAN** section, information about the **2.4GHz** Wireless Local Area Network configuration is displayed.

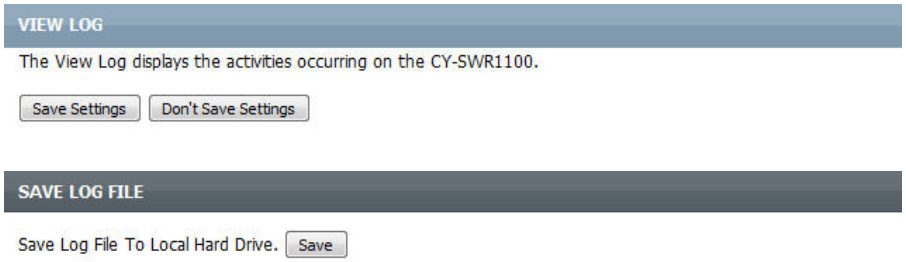


In the **Wireless LAN2** section, information about the **5GHz** Wireless Local Area Network configuration is displayed.



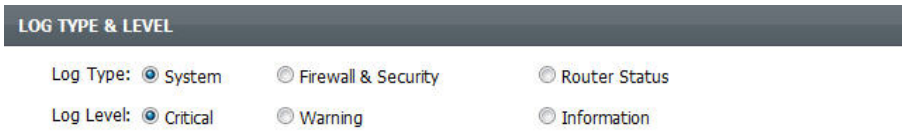
Logs

The router automatically logs (records) events of possible interest in it's internal memory. If there isn't enough internal memory for all events, logs of older events are deleted but logs of the latest events are retained. The Logs option allows you to view the router logs. You can define what types of events you want to view and the level of the events to view. This router also has external Syslog Server support so you can send the log files to a computer on your network that is running a Syslog utility.



You can configure the following parameters:

Save Log File:	Click the **Save** button to save the Router's log entries to a log file on your computer.



You can configure the following parameters:

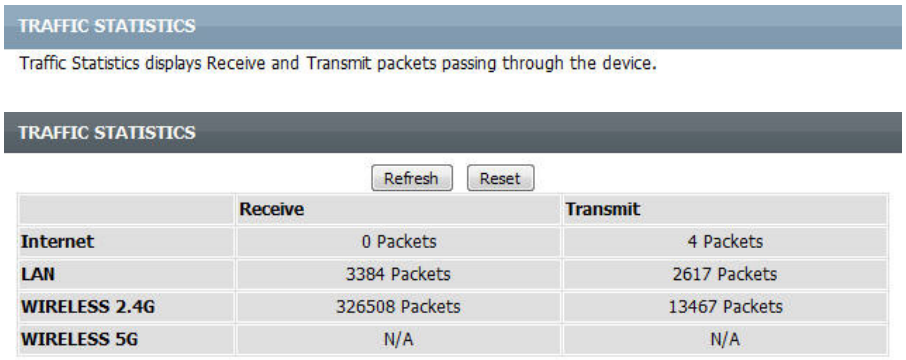
Log Type:	Use the radio buttons to select the types of messages that you want to display from the log. You can select System, Firewall & Security, and Router Status messages.
Log Level:	There are three levels of message importance: Critical, Warning, and Information. Select the levels that you want displayed in the log.

You can configure the following parameters:

First - Last Page:	Use these buttons to navigate to the first or last page of the router logs.
Previous - Next:	Use these buttons to navigate to the next or previous page of the router logs.
Clear:	Click this button to clear all the contents from the log.
Link to Email Log Settings:	Click this button to open the Email Settings screen so that you can change the Email configuration for sending logs.

Statistics

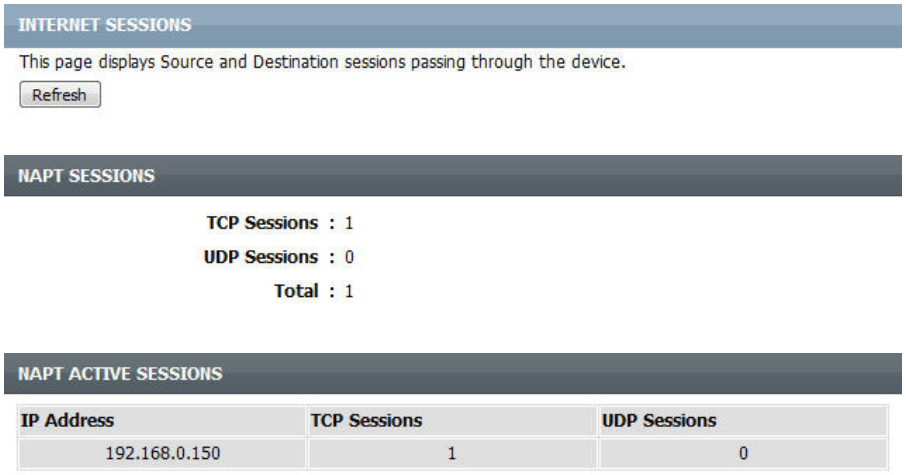
The screen below displays the Traffic Statistics. You can view the number of packets that pass through the router on both the WAN and LAN ports and both the 802.11n/g (2.4GHz) and 802.11n/a (5GHz) wireless bands. The traffic counter will reset if the device is rebooted.



Click the **Refresh** button to refresh the display page.
Click the **Reset** button to clear all the statistics for all the fields displayed.

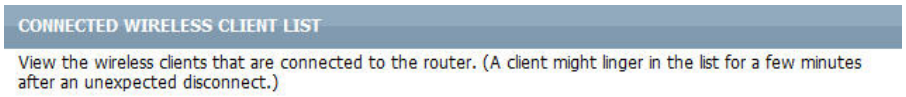
Internet Sessions

The Internet Sessions page displays full details of active Internet sessions through your router. An Internet session is a conversation between a program or application on a LAN-side computer and a program or application on a WAN-side computer.



Wireless

The wireless client table displays a list of current connected wireless clients. This table also displays the connection time and MAC address of the connected wireless clients.

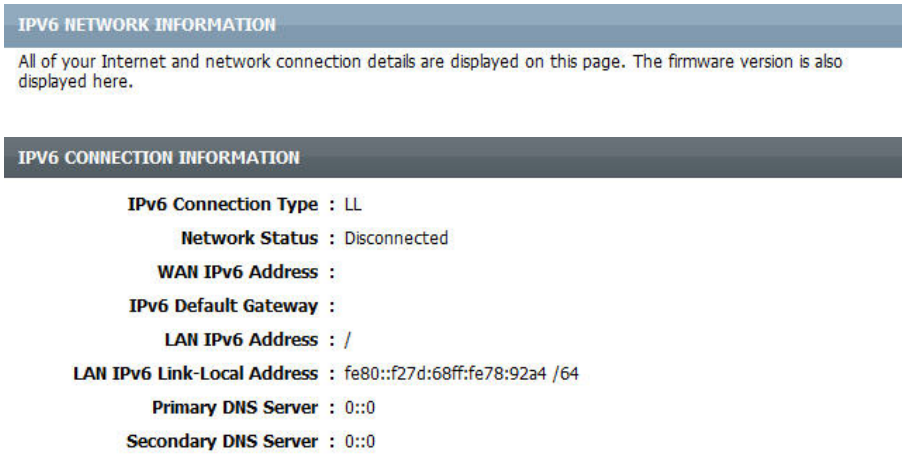


In the **Number of Wireless Clients - 2.4GHz Band** section a list of 2.4GHz active wireless clients will be displayed.

In the **Number of Wireless Clients - 5GHz Band** section a list of 5GHz active wireless clients will be displayed.

IPv6

The IPv6 page displays a summary of the Router's IPv6 settings and lists the IPv6 address and host name of any IPv6 clients.



Support Tab

The Support Tab gives you access to basic information about each page and parameter that exists on this device.

Special Features of the CY-SWR1100

One Foot Connection

The One Foot Connection function lets you connect your One Foot Connection compliant Samsung TV automatically to the Samsung CY-SWR1100 wireless router.

* One Foot Connection is only supported by some Samsung TV/AV/Touch Control products made in 2011 and after. Each product has a different way of using One Foot Connection. For more information, see the manual for each product.
* When WPS is disabled, OFC function will not work.

To connect a Samsung TV using One Foot Connection, follow these steps:

1. Turn on the Samsung wireless router and the TV.
2. Go to Network Settings screen. (MENU → Network → Network Settings → ENTER.)
3. Select One Foot Connection, and press ENTER, then press ENTER again.
4. Place the wireless router in parallel with your TV set, and no farther away than 25cm (about 9 3/4 inches).

   Note: If One Foot Connection does not connect your TV to your router, a pop-up window appears on the screen notifying you of the failure. If you want to try using One Foot Connection again, reset the wireless router, and then try again from Step 1. You can also choose one of the other connection setup methods.
5. The network connection screen appears, and network setup is complete.
6. Move the wireless router to a desired location.

   Note: If the wireless router's settings change or you install a new wireless router, you must perform the One Foot Connection procedure again, beginning from Step 1.

Plug & Access

The Plug & Access function lets you easily connect your Plug & Access compliant Samsung TV to your Samsung wireless router by using a USB memory stick to transfer the setup information from the router to the TV.

* Plug & Access is only supported by some Samsung TVs made in 2011 and after. For more information, see the manual of the individual TV.

***USB flash memory Requirements**
File system - FAT16 or FAT32
Free space - 2KB (Minimum)

Connecting...

Connected!

To connect a Samsung TV using Plug & Access, follow these steps:

1. Turn on the Samsung wireless router and your TV.
2. Insert a USB memory stick into the USB port in your Samsung wireless router. Check the router's LED's to make sure it is on (Blinking → on).
3. About a minute later, take the USB memory stick out of the router, and then insert it into a USB port on your Samsung TV. The memory stick downloads the connection information.
4. Wait until the connection is automatically established.

   Note: If Plug & Access does not connect your TV to your wireless router, a pop-up window appears on the screen notifying you of the failure. If you want to try using Plug & Access again, reset the AP, disconnect the Samsung Wireless LAN adapter and then try again from Step 1. You can also choose one of the other connection setup methods.
5. The network connection screen appears, and the network setup is complete.
6. Place the wireless router in a desired location.

Notes:

- If the wireless router's settings change or you install a new wireless router, you must perform the Plug & Access procedure again, beginning from Step 1.
- After the connection data transfer has been completed, the WPS light on the router glows continuously.

Priority QoS

Samsung wireless routers are optimized to stream HD AV to Samsung TV / BDP.

* Priority QoS is only supported by some Samsung TVs and Blu-ray players made in 2011 and after. For more information, see the manual of the individual unit.

The Priority QoS function is unique to the CY-SWR1100.

You can connect a Samsung wireless router to many devices, such as laptops, mobile phones, BD players etc. However, when you connect a Samsung TV or Blu-ray player to a Samsung wireless router, the Samsung wireless router gives the Samsung TV or player a priority connection. This ensures your TV or player gets the fastest throughput speed and displays the highest quality streaming contents.

* The way how to set up Priority QoS in CY-SWR1100 is on the next page.

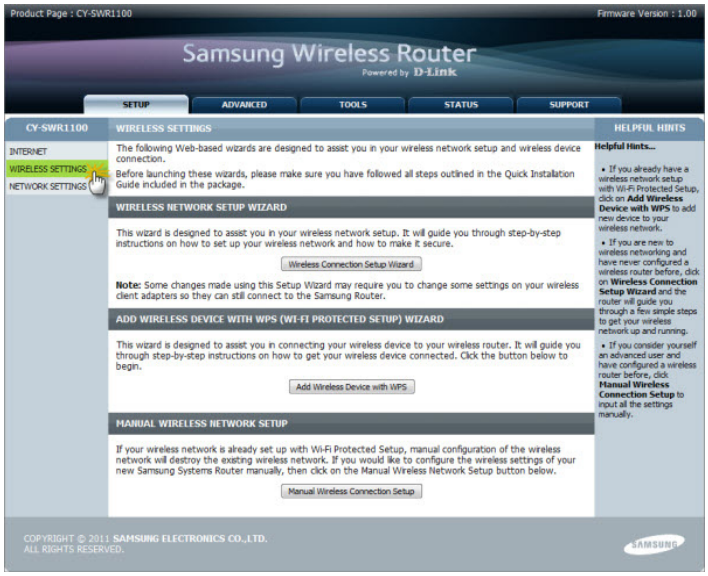
How to set up PRIORITY QoS

Step 1

Connect to your wireless router's Web User Interface. (For more information, go to "Connecting to the Web UI" on page 11 in this manual.)

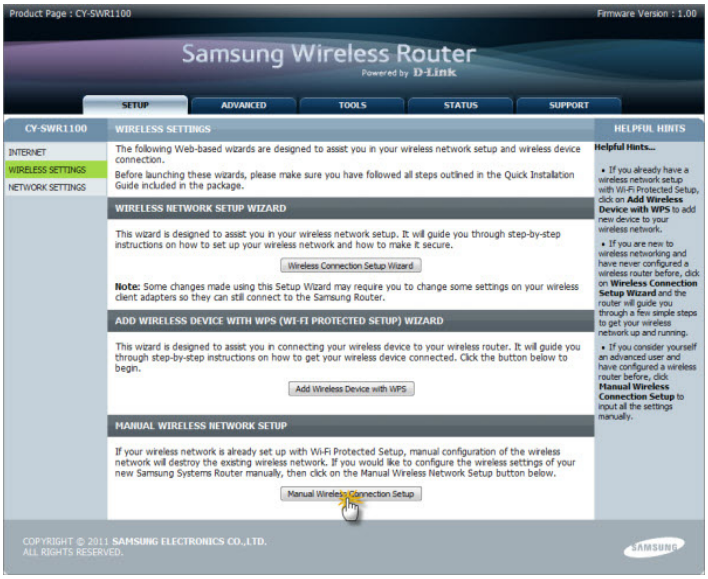
Step 2

Click **WIRELESS SETTINGS** in the SETUP Tap.



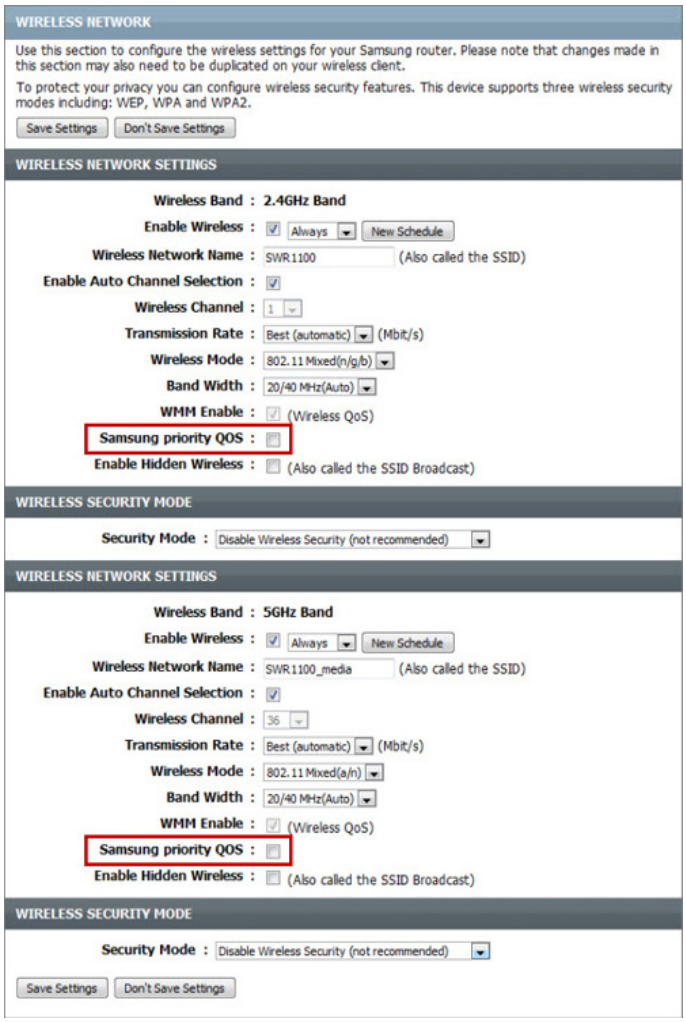
Step 3

Click the **Manual Wireless Connection Setup** button.



Step 4

Check the **Samsung priority QOS** box for each wireless band.



Step 5

Click the **Save Settings** button to accept the changes.

Wireless Basics

Wireless products are based on industry standards designed to provide easy-to-use and compatible high-speed wireless connectivity within your home, business or public access wireless networks. Strictly adhering to the IEEE standard, Samsung the wireless family of products will allow you to access the data you want securely, when and where you want it. You will be able to enjoy the freedom that wireless networking delivers.

A wireless local area network (WLAN) is a cellular computer network that transmits and receives data with radio signals instead of wires. Wireless LANs are used increasingly in both home and office environments, and public areas such as airports, coffee shops and universities. Innovative ways to utilize WLAN technology are helping people to work and communicate more efficiently. Increased mobility and the absence of cabling and other fixed infrastructure have proven to be beneficial for many users.

Wireless users can use the same applications they use on a wired network. Wireless adapter cards used on laptop and desktop systems support the same protocols as Ethernet adapter cards.

Under many circumstances, it is desirable for mobile network devices to link to a conventional Ethernet LAN to use servers, printers or an Internet connection supplied through the wired LAN. Samsung's Wireless Router provides this link.

What is Wireless?

Wireless or Wi-Fi technology is another way of connecting your computer to the network without using wires. Wi-Fi uses radio frequency to connect wirelessly, so you have the freedom to connect computers anywhere in your home or office network.

How does Wireless work?

Wireless networking works much the same way as cordless phone work, through radio signals that transmit data from one point A to point B. But wireless technology has restrictions which limit how you can access the network. You must be within the wireless network's range to be able to connect your computer.

Wireless Local Area Network (WLAN)

There are two different types of wireless networks: Wireless Local Area Network (WLAN), and Wireless Personal Area Network (WPAN).

In a wireless local area network, a device called an Access Point (AP) connects computers to the network. The access point has a small antenna attached to it, which allows it to transmit data back and forth using radio signals. With an indoor access point, the signal can travel up to 300 feet. With an outdoor access point, the signal can reach out up to 30 miles and serve places such as manufacturing plants, industrial locations, college and high school campuses, airports, golf courses, and many other outdoor venues.

Wireless Personal Area Network (WPAN)

Bluetooth is the industry standard wireless technology used for WPAN. Bluetooth devices in WPANs have a range of up to 30 feet. Compared to WLAN, the speed and wireless operation range are less, but in return, Bluetooth doesn't use nearly as much power which makes it ideal for personal devices, such as mobile phones, PDAs, headphones, laptops, speakers, and other devices that operate on batteries.

Who uses wireless?

Wireless technology has become so popular in recent years that almost everyone is using it. Whether it's for home, office, business, Samsung has a wireless solution for it.

Benefits in the Home

- Gives everyone at home broadband access
- Surf the web, check email, instant message, etc.
- Gets rid of the cables around the house
- Simple and easy to use

Benefits for a Small Office and Home Office

- Stay on top of everything at home as you would at the office
- Remotely access your office network from home
- Share one Internet connection and printer with multiple computers
- No need for dedicated office space

Where is wireless used?

Wireless technology is expanding everywhere, not just at home or office. People like the freedom of mobility and it's becoming so popular that more and more public facilities now provide wireless access to attract people. The wireless connections in public places are usually called "hotspots".

Using a Wireless Cardbus Adapter with your laptop, you can access the hotspot to connect to the Internet from remote locations such as airports, hotels, coffee shops, libraries, restaurants, and convention centers.

Setup Tips

A wireless network is easy to setup, but if you're installing it for the first time, it could be quite a task if you don't know where to start. That's why we've put together a few setup steps and tips to help you through the process of setting up a wireless network.

Centralize your router or access point

Make sure you place the router/access point in a centralized location within your network for the best performance. Try to place the router/access point as high as possible in the room, so the signal gets dispersed throughout your home. If you have a two-story home, you may need a repeater to boost the signal to extend the range.

Eliminate Interference

Place home appliances such as cordless telephones, microwaves, and televisions as far away as possible from the router/access point. This would significantly reduce any interference that the appliances might cause since they operate on same frequency.

Security

Don't let you next-door neighbors or intruders connect to your wireless network. Secure your wireless network by turning on the WPA or WEP security feature on the router. Refer to product manual for detailed information on how to set it up.

Wireless Modes

There are basically two modes of networking:

- Infrastructure – All wireless clients will connect to an access point or wireless router.
- Ad-Hoc – Directly connecting to another computer, for peer-to-peer communication, using wireless network adapters on each computer, such as two or more wireless network Cardbus adapters.

An Infrastructure network contains an Access Point or wireless router. All the wireless devices, or clients, will connect to the wireless router or access point.

An Ad-Hoc network contains only clients, such as laptops with wireless cardbus adapters. All the adapters must be in Ad-Hoc mode to communicate.

Wireless Security

This section explains the different levels of security you can use to protect your data from intruders. Your Samsung router offers wireless security options such as WPA/WPA2 PSK/EAP.

What is WPA?

WPA (Wi-Fi Protected Access) is a Wi-Fi standard that was designed to improve the security features of WEP (Wired Equivalent Privacy).

The 2 major improvements over WEP:

- Improved data encryption through the Temporal Key Integrity Protocol (TKIP). TKIP scrambles the keys using a hashing algorithm and, by adding an integrity-checking feature, ensures that the keys haven't been tampered with. WPA2 is based on 802.11i and uses Advanced Encryption Standard (AES) instead of TKIP.
- User authentication, which is generally missing in WEP, through the extensible authentication protocol (EAP). WEP regulates access to a wireless network based on a computer's hardware-specific MAC address, which is relatively easy sniff out and steal. EAP is built on a more secure public-key encryption system to ensure that only authorized network users can access the network.

WPA-PSK/WPA2-PSK uses a passphrase or key to authenticate your wireless connection. The key is an alpha-numeric password between 8 and 63 characters long. The password can include symbols (!?*&_) and spaces. This key must be the exact same key entered on your wireless router or access point.

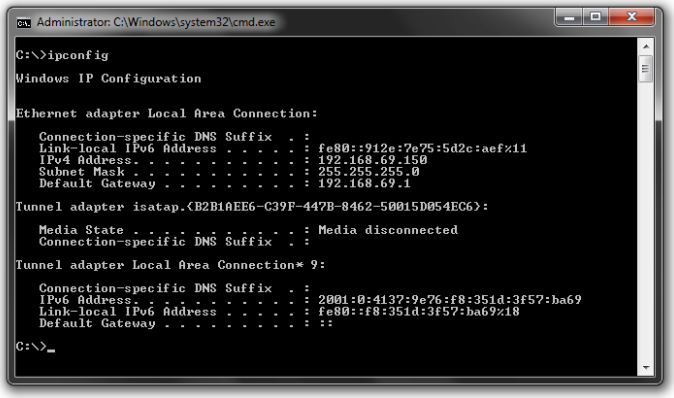
WPA/WPA2 incorporates user authentication through the Extensible Authentication Protocol (EAP). EAP is built on a more secure public key encryption system to ensure that only authorized network users can access the network.

Networking Basics

Check your IP address

After you install your new network or wireless adapter, by default, the TCP/IP settings should be set to obtain an IP address from a DHCP server (i.e. wireless router) automatically. To verify your IP address, please follow the steps below.

1. Click Start > Run.
2. In the run box, type cmd and click OK. (Windows® 7/Vista® users type cmd in the Start Search box.)
3. At the prompt, type ipconfig, and then press Enter.



This will display the IP address, subnet mask, and the default gateway of your adapter.

If the address is 0.0.0.0, check your adapter installation, security settings, and the settings on your router. Some fire-wall software programs may block a DHCP request on newly installed adapters.

Statically Assign an IP address

If you are not using a DHCP capable gateway/router, or you need to assign a static IP address, please follow the steps below:

Step 1

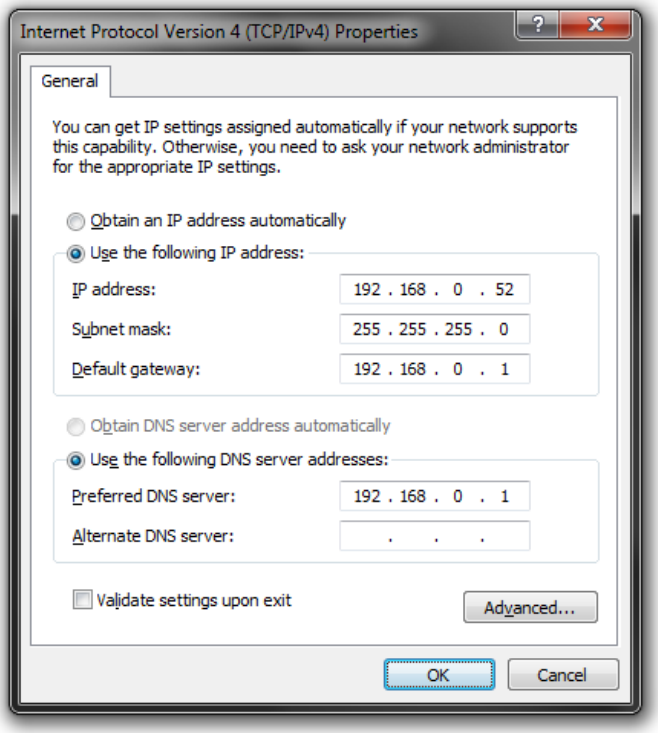
- Windows® 7 - Click Start > Control Panel > Network and Internet > Network and Sharing Center > Change Adapter Setting.
- Windows Vista® - Click Start > Control Panel > Network and Internet > Network and Sharing Center > Manage Network Connections.
- Windows® XP - Click Start > Control Panel > Network Connections.
- Windows® 2000 - From the desktop, right-Click My Network Places > Properties.

Step 2

Right-Click the Local Area Connection which represents your network adapter and select Properties.

Step 3

Highlight Internet Protocol (TCP/IP) and Click Properties.



Step 4

Click “Use the following IP address”, and then enter an IP address that is on the same subnet as your network or the LAN IP address on your router.

Example: If the router’s LAN IP address is 192.168.0.1, make your IP address 192.168.0.X where X is a number between 2 and 99. Make sure that the number you choose is not in use on the network. Set Default Gateway to the same value as the LAN IP address of your router (192.168.0.1).

Set Primary DNS to the same value as the LAN IP address of your router (192.168.0.1). The Secondary DNS is not needed or you may enter a DNS server from your ISP.

Step 5

Click OK twice to save your settings.

Connect to a Wireless Network

Using Windows® 7

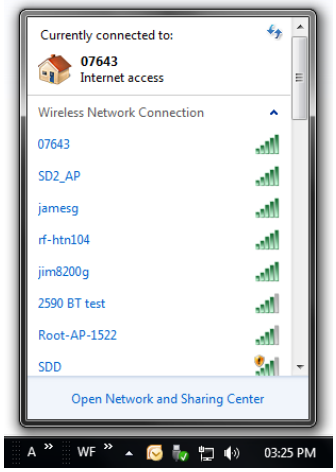
We recommended that you enable wireless security (WPA/WPA2) on your wireless router or access point before configuring your wireless adapter. If you are adding the computer to an existing network with security, you will need the network's security key key or passphrase being used.

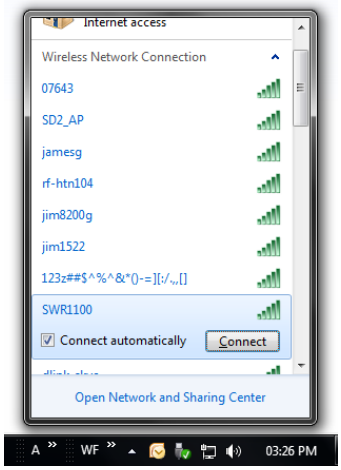
1. Click the wireless icon in your system tray. (lower-right corner).

2. The utility will display any available wireless networks in your area.

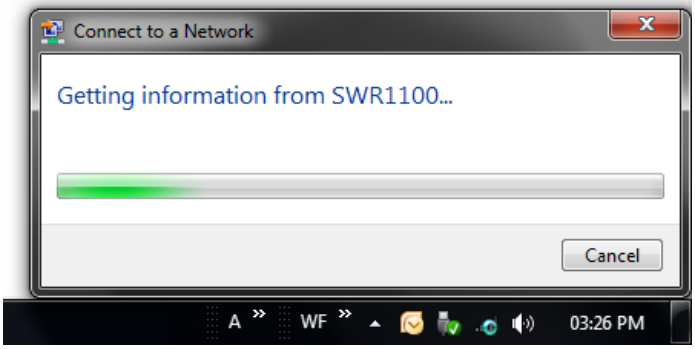
3. Highlight the wireless network (SSID) you would like to connect to, and then Click the Connect button.

If you get a good signal but cannot access the Internet, check the TCP/IP settings for your wireless adapter. Refer to the Networking Basics section in this manual for more information.



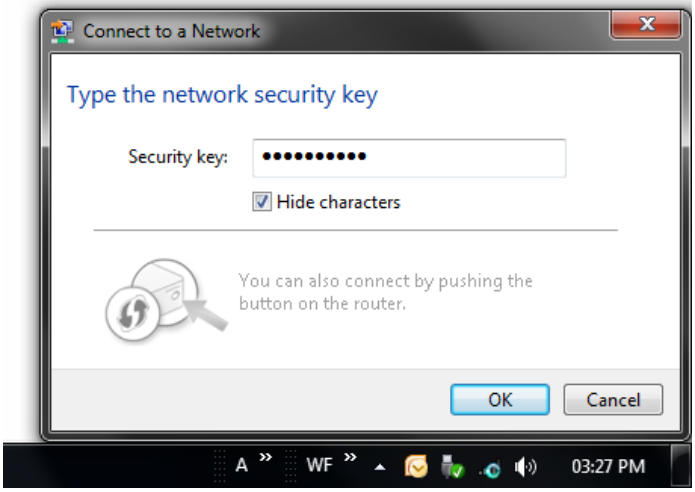


4. The following window appears while your computer tries to connect to the router.



5. Enter the same security key or passphrase that is on your router and Click Connect. You can also connect by pushing the WPS button on the router.

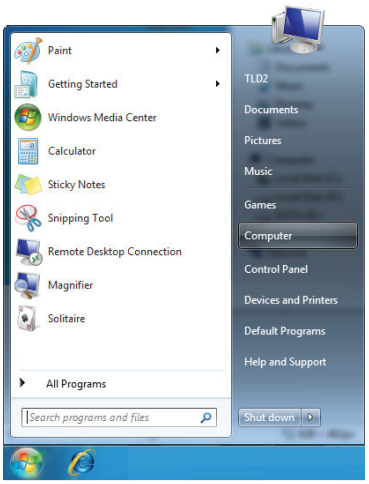
It may take 20-30 seconds to connect to the wireless network. If the connection fails, please verify that the security settings are correct. The key or passphrase must be exactly the same as on the wireless router.



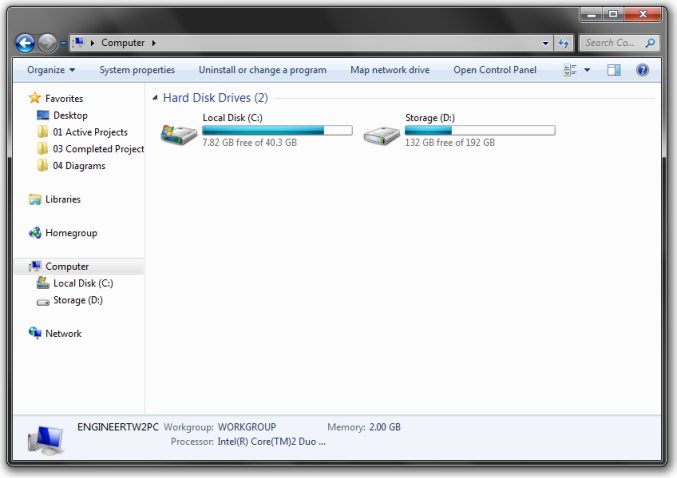
Configuring WPS

You can configure the WPS feature of the router using Windows® 7. Follow the steps below to use Windows® 7 to configure the WPS feature of the router:

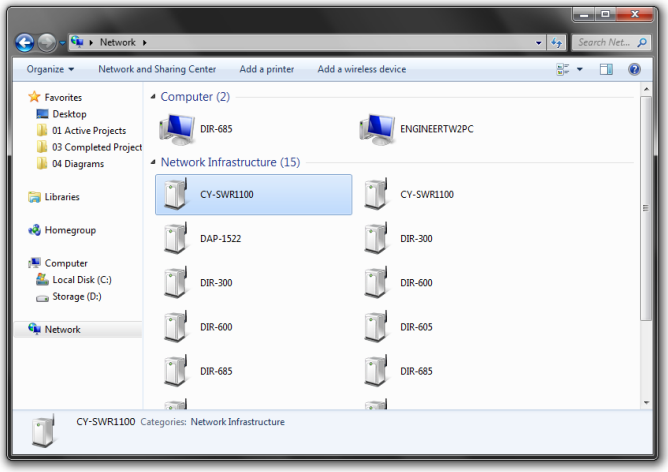
1. Click the Start button, and select then Computer from the Start menu.



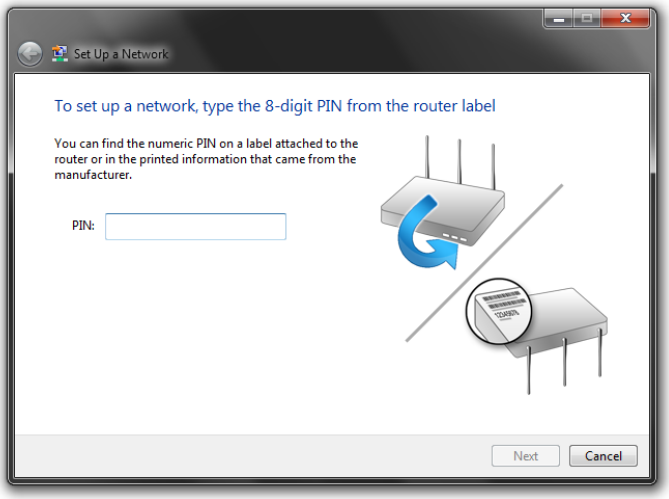
2. Click the Network option.



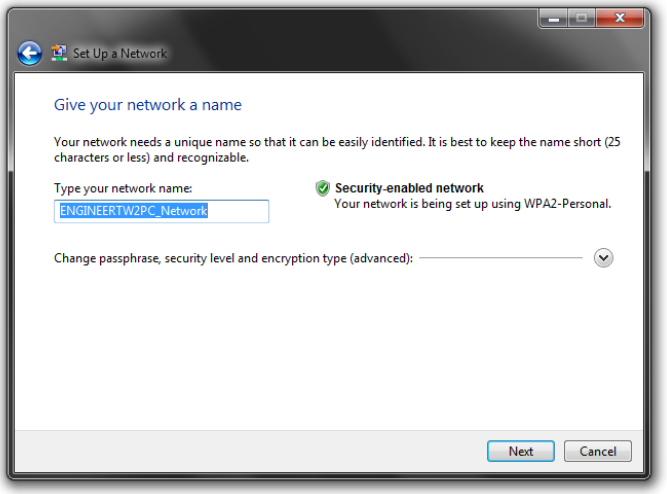
3. Double-Click the Router.



4. Input the WPS PIN number, and then click Next.

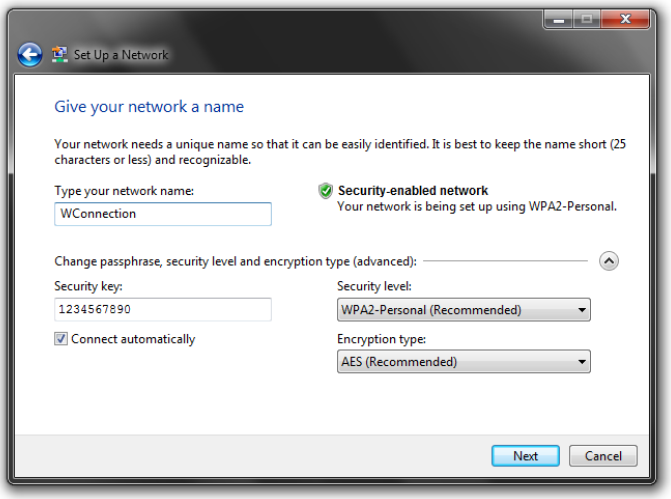


5. Type a name to identify the network.



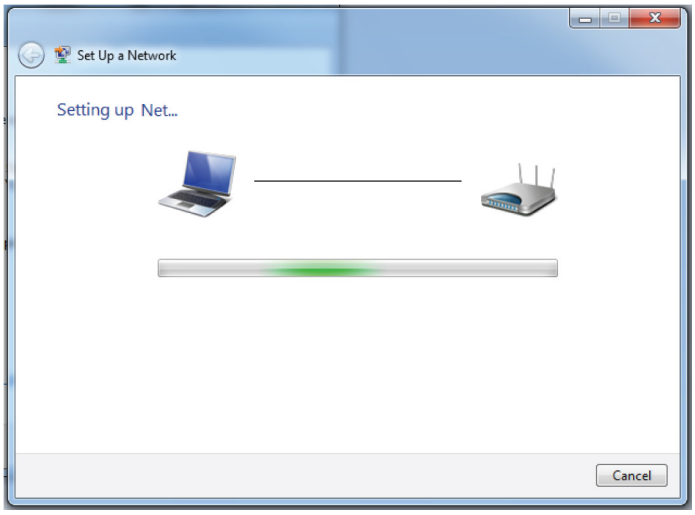
6. To configure advanced settings, click the drop-down icon.

Click Next to continue.



7. The following window appears while the Router is being configured.

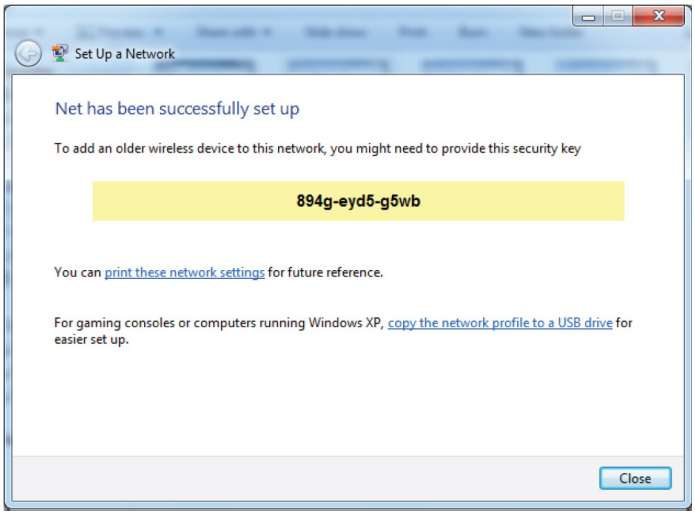
Wait for the configuration to complete.



8. The following window informs you that WPS on the CY-SWR1100 has been setup successfully.

Make a note of the security key. You may need to provide this security key if adding an older wireless device to the network in the future.

9. Click Close to complete WPS setup.

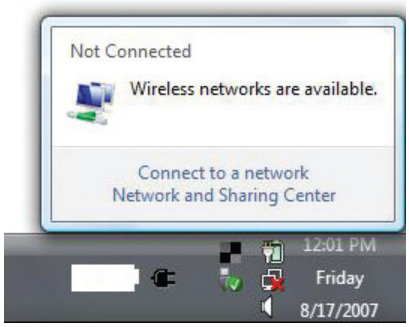


Using Windows Vista®

Windows Vista® users may use the built-in wireless utility. If you are using another company's utility or Windows® 2000, please refer to You manual of your wireless adapter for help with connecting to a wireless network. Most utilities will have a "site survey" option similar to the Windows Vista® utility as seen below.

1. If you see the Wireless Networks Detected pop-up, click the center of the pop-up to access the utility or right-Click the wireless computer icon in your system tray (lower-right corner next to the time).

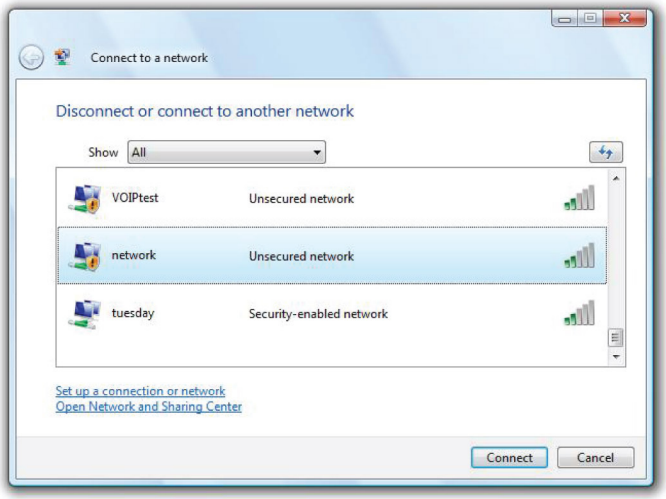
2. Select Connect to a network.



3. The utility will display any available wireless networks in your area.

4. Click a network (displayed using the SSID), and then Click the Connect button.

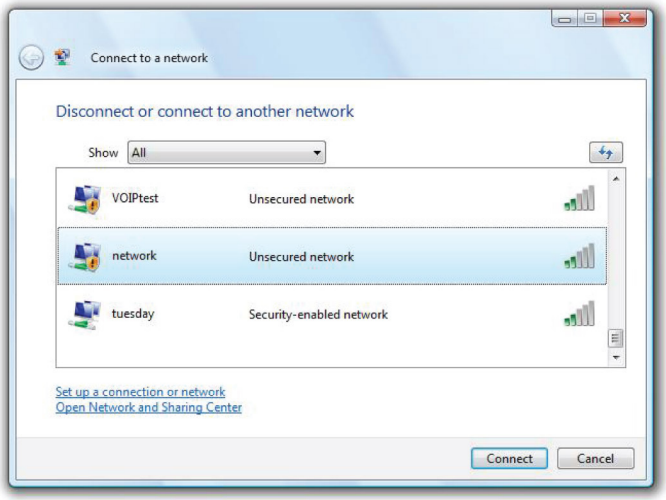
5. If you get a good signal but cannot access the Internet, check you TCP/IP settings for your wireless adapter. Refer to the Networking Basics section in this manual for more information.



We recommend that you enable wireless security (WPA/WPA2) on your wireless router or access point before configuring your wireless adapter. If you are joining an existing network, you will need to know the security key or passphrase being used.

1. Open the Windows Vista® Wireless Utility by right-clicking the wireless computer icon in your system tray (lower right corner of screen). Select Connect to a network.

2. Highlight the wireless network (SSID) you would like to connect to, and then click Connect.



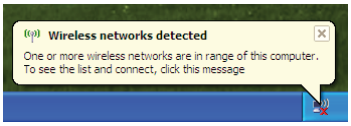
3. Enter the same security key or passphrase that is on your router, and then click Connect.

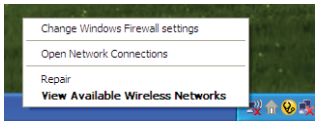
It may take 20-30 seconds to connect to the wireless network. If the connection fails, please verify that the security settings are correct. The key or passphrase must be exactly the same as on the wireless router.

Using Windows® XP

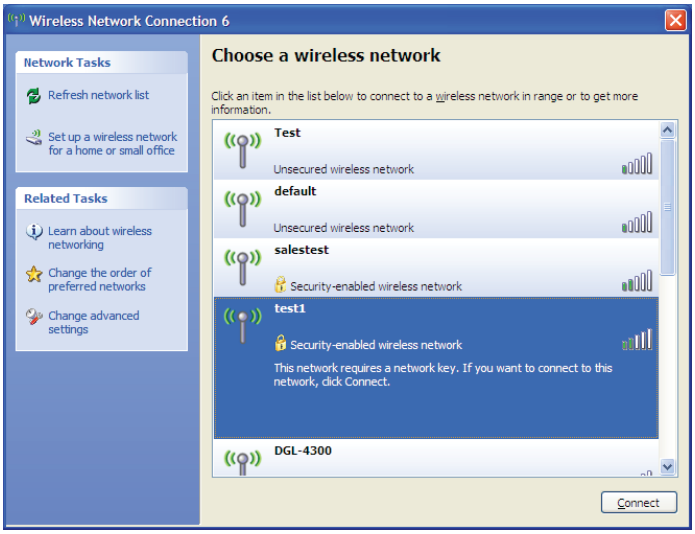
Windows® XP users may use the built-in wireless utility (Zero Configuration Utility). The following instructions are for Service Pack 2 users. If you are using another company's utility or Windows® 2000, please refer to You manual of your wireless adapter for help with connecting to a wireless network. Most utilities will have a "site survey" option similar to the Windows® XP utility as seen below.

If you receive the Wireless Networks Detected pop-up, click the center of the pop-up to access the utility or right-Click the wireless computer icon in your system tray (lower right corner next to the time). Select View Available Wireless Networks.





The utility will display any available wireless networks in your area. Click a network (displayed using the SSID), and then Click the Connect button.

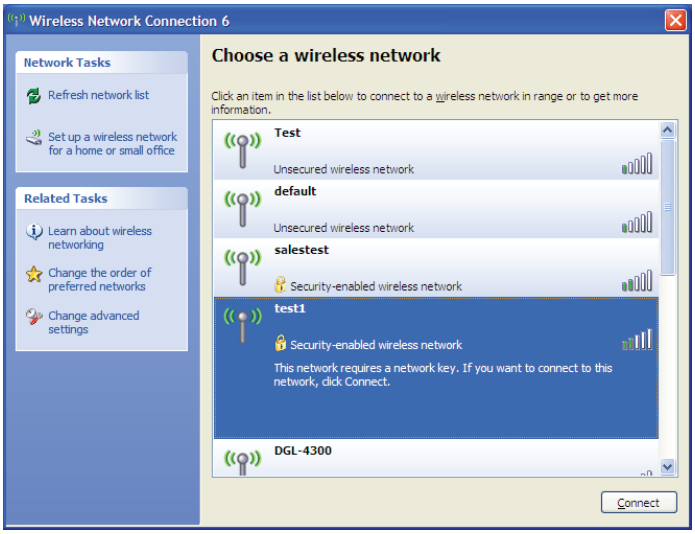


If you get a good signal but cannot access the Internet, check you TCP/ IP settings for your wireless adapter. Refer to the Networking Basics section in this manual for more information.

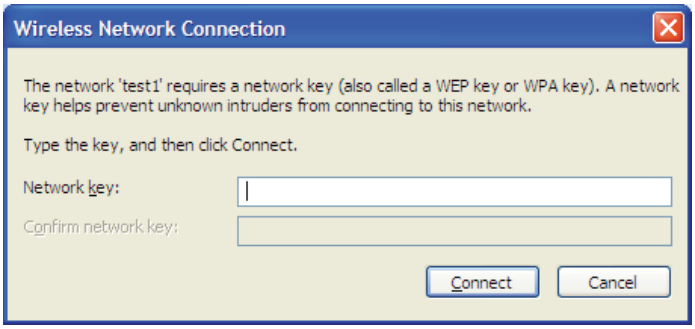
We recommend that you enable WPA wireless security on your wireless router or access point before configuring your wireless adapter. If you are joining an existing network, you will need to know the WPA key being used.

1. Open the Windows® XP Wireless Utility by right-clicking the wireless computer icon in your system tray (lower-right corner of screen). Select View Available Wireless Networks.

2. Highlight the wireless network (SSID) you would like to connect to, and then click Connect.



3. The Wireless Network Connection box will appear. Enter the WPA-PSK passphrase, and then click Connect.



It may take 20-30 seconds to connect to the wireless network. If the connection fails, please verify that the WPA-PSK settings are correct. The WPA-PSK passphrase must be exactly the same as on the wireless router.

TROUBLESHOOTING

This chapter provides solutions to problems that can occur during the installation and operation of the router. Read the following descriptions if you are having problems. The examples below are based on Windows® XP. If you have a different operating system, the procedures will be similar.

Why can't I access the router's web-based configuration utility (Web UI)?

When entering the IP address of the router (192.168.0.1 for example), you are not connecting to a website nor do you have to be connected to the Internet. The device has the utility built-in to a ROM chip in the device itself that displays the router's configuration utility through your browser. Your computer, through, must be on the same IP subnet to connect to the web-based utility.

Make sure you have an updated Java-enabled web browser. We recommend the following:

- Microsoft Internet Explorer® 6.0 and higher
- Mozilla Firefox 3.0 and higher
- Google™ Chrome 2.0 and higher
- Apple Safari 3.0 and higher

Verify physical connectivity by checking for solid link lights on the router. If you do not get a solid link light, try using a different cable or connect to a different port on the device if possible. If the computer is turned off, the link light may not be on.

Disable any Internet security software running on the computer. Software firewalls such as Zone Alarm, Black Ice, Sygate, Norton Personal Firewall, and Windows® XP firewall may block access to the configuration pages. Check the help files included with your firewall software for more information on disabling or configuring it.

Configure your Internet settings:

- Go to Start > Settings > Control Panel. Double-Click the Internet Options Icon. From the Security tab, click the button to restore the settings to their defaults.
- Click the Connection tab and set the dial-up option to Never Dial a Connection. Click the LAN Settings button. Make sure nothing is checked. Click OK.
- Go to the Advanced tab and Click the button to restore these settings to their defaults. Click OK three times.
- Close your web browser (if open) and open it.

Try accessing the Web UI again. Open your web browser and enter the IP address of your router in the address bar. This should open the login page for your Web UI.
If you still cannot access the configuration utility, unplug the power to the router for 10 seconds and plug back in. Wait about 30 seconds and try accessing the configuration. If you have multiple computers, try connecting using a different computer.

What can I do if I forgot my password?

If you forgot your password, you must reset your router. Unfortunately this process will change all your settings back to the factory defaults.

To reset the router, locate the reset button (hole) on the rear panel of the unit. With the router powered on, use a paperclip to hold the button down for 10 seconds. Release the button and the router will go through its reboot process. Wait about 30 seconds to access the router. The default IP address is 192.168.0.1. When logging in, the username is admin. Leave the password box empty.

Why can't I connect to certain sites or send and receive e-mails when connecting through my router?

If you are having a problem sending or receiving email, or connecting to secure sites such as eBay, banking sites, and Hotmail, we suggest lowering the MTU in increments of ten (Ex. 1492, 1482, 1472, etc).

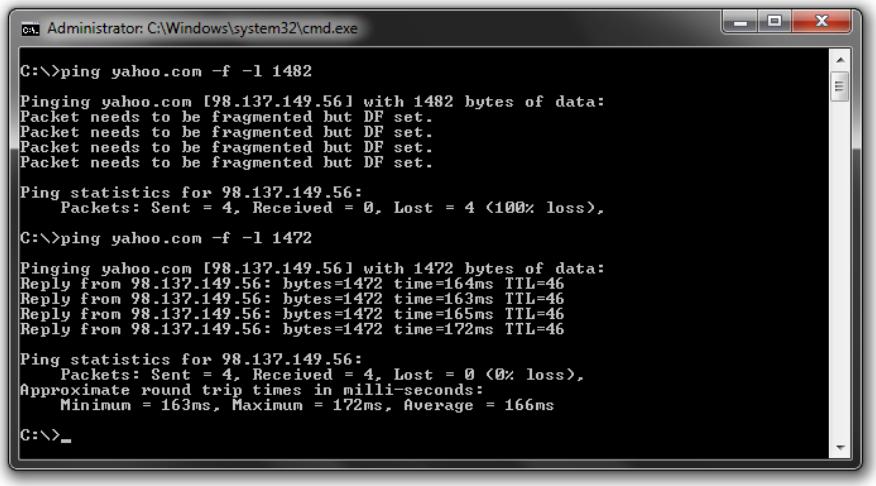
To find the proper MTU Size, you'll have to do a special ping of the destination you're trying to go to. A destination could be another computer or a URL.

⚠	**Note:** AOL DSL+ users must use MTU of 1400.

- Click Start and then Click Run.
- Windows® 95, 98, and Me users type in command (Windows® NT, 2000, and XP users type in cmd) and press Enter (or Click OK).
- Once the window opens, you'll need to do a special ping. Use the following syntax: ping [url] [-f] [-l] [MTU value]

Example: ping yahoo.com -f -l 1472

You should start at 1472 and work your way down by 10 each time. Once you get a reply, go up by 2 until you get a fragmented packet. Take that value and add 28 to account for the various TCP/IP headers. For example, lets say that 1452 was the final value. The actual MTU size would be 1480, which is the optimum for the network we're working with (1452+28=1480).



Once you find your MTU, you can now configure your router with the proper MTU size.

To change the MTU rate on your router follow the steps below:

1. Open your browser, enter the IP address of your router (192.168.0.1), and Click then OK.
2. Enter your username (admin) and password (blank by default). Click OK to enter the web configuration page for the device.
3. Click Setup, and then click Manual Configure.
4. To change the MTU, enter the number in the MTU field, and then click Save Settings to save your settings.
5. Test your email. If changing the MTU does not resolve the problem, continue changing the MTU in increments of ten.

Technical Specifications

Hardware Specifications

WAN Interface:
- 1 x 10/100/1000Mbps WAN - Auto MDI/MDIX

LAN Interface:
- 4 x 10/100/1000Mbps PC Port - Auto MDI/MDIX

Wireless Interface:
- 802.11a/b/g/n (Simultaneous)

Status LEDs:
- Power, WAN, Wireless(2.4GHz/5GHz), WPS, LAN, USB

Temperature:
- Operating: 50 ~ 104°F (10 ~ 40°C)
- Storing: -4 ~ 113°F (-20 ~ 45°C)

Operating Voltage:
- Input: 100~240V (±20%), 50~60Hz
- Output: DC12V, 2A

Software Specifications

NAT:
- PNAT

Protocols:
- HTTP, DHCP, PPPoE, PPTP, L2TP

Application Protocol:
- H323, MSN, BattleNet, etc

QoS:
- TV Priority QoS

Function Control:
- PC-based Console management

Wireless Connection:
- One Foot Connection, Plug & Access

Wireless Specifications:

Standards:
- IEEE 802.11a, IEEE 802.11b, IEEE 802.11g, IEEE 802.11n

Wireless Frequency Range:
- 2.4GHz (2.4GHz ~ 2.4835GHz)
- 5GHz (5.15GHz ~ 5.25GHz, 5.725GHz ~ 5.850GHz)

MIMO:
- 2Tx and 2Rx

Wireless Bandwidth Rate:
- IEEE 802.11a : 6, 9, 12, 18, 24, 36, 48, 54Mbps
- IEEE 802.11b : 1, 2, 5.5, 11Mbps
- IEEE 802.11g : 6, 9, 12, 18, 24, 36, 48, 54Mbps
- IEEE 802.11n : MAX 300Mbps (with HT40MHz)

RF Output Power:
- 802.11a - 7-17dBm
- 802.11b - 15-19dBm
- 802.11g - 12-18dBm
- 802.11n - 6-16dBm

Modulation:
- OFDM (BPSK, QPSK, 16QAM, 64QAM), DSSS (BPSK, DQPSK, CCK)

Wireless Security:
- 64/128bit WEP
- WPA-PSK
- WPA2-PSK
- WPA-PSK/WPA2-PSK
- WPS (PIN & PBC)

Warranty

Period:
- 2 years

Dimension

Set Size:
- 167 x 83 x 140 mm (WxDxH) (mm)
- (6.57 x 3.27 x 5.51 in)

Package:
- 274 x 68 x 208 mm (WxDxH) (mm)
- (10.79 x 2.67 x 8.19 in)

Weight

Product Weight:
- 349.8 gram
- (11.83 oz)

Package Weight:
- 705.7 gram
- (23.86 oz)

Accessory

Contents:
- Installation CD
- Quick Install Guide
- Power Adaptor with Power Cord
- LAN Cable
- Stand
- Wall Mount Kit

Regulatory Compliance Information

FCC Compliance Statement

This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions:
(1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

Interference

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, You is encouraged to try to correct the interference by one of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

Wireless Radio

For product available in the USA/Canada market, only channel 1~11 can be operated. Selection of other channels is not possible. This device is going to be operated in 5.15~5.25GHz frequency range, it is restricted in indoor environment only.
Important: Changes or modifications not expressly approved by the party responsible for compliance could void You's authority to operate the equipment.
FCC Radiation Exposure Statement: This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20cm between the radiator and your body.

Industry Canada Statement

This Class B digital apparatus complies with Canadian ICES-003.
Cet appareil numérique de la classe B est conforme à la norme NMB-003 du Canada.
Operation is subject to the following two conditions:
(1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.
This device and its antenna(s) must not be collocated or operation in conjunction with any other antenna or transmitter.

Wireless Radio

For product available in the USA/Canada market, only channel 1~11 can be operated. Selection of other channels is not possible.
The device could automatically discontinue transmission in case of absence of information to transmit, or operational failure. Note that this is not intended to prohibit transmission of control or signalling information or the use of repetitive codes where required by the technology.
Important: Changes or modifications not expressly approved by the party responsible for compliance could void You's authority to operate the equipment.
IC Radiation Exposure Statement: This equipment complies with IC RSS-102 radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20cm between the radiator & your body.

Dispose unwanted electronics through an approved recycler.
To find the nearest recycling location, go to our website:
www.samsung.com/recyclingdirect Or call, (877) 278 - 0799